Contents

CAPITOLUL 2. NETWORK THREATS 3

2.0 Introduction 3

2.0.1 – Scope 3

2.0.2 - Obiectiv 3

2.1 Who is Attacking Our Network? 3

2.1.1 - Threat, Vulnerability, and Risk 3

2.1.2 - Hacker vs. Threat Actor 5

2.1.3 - Evolution of Threat Actors 6

2.1.4 - Cybercriminals 7

2.1.5 - Cybersecurity Tasks 7

2.1.6 - Cyber Threat Indicators 8

2.1.7 - Threat Sharing and Building Cybersecurity Awareness 9

2.2 Threat Actor Tools 11

2.2.1 - Introduction of Attack Tools 11

2.2.2 - Evolution of Security Tools 12

2.2.3 - Categories of Attacks 13

2.3 Malware 15

2.3.1 - Types of Malware 15

2.3.2 - Viruses 15

2.3.3 - Trojan Horses 15

2.3.4 - Trojan Horse Classification 16

2.3.6 - Worm Components 18

2.3.7 - Ransomware 19

2.3.8 - Other Malware 20

2.3.9 - Common Malware Behaviors 21

2.4 Common Network Attacks - Reconnaissance, Access, and Social Engineering 23
2.4.1 - Types of Network Attacks 23
2.4.2 - Reconnaissance Attacks 23
2.4.3 - Access Attacks 24
2.4.4 - Social Engineering Attacks 25
2.4.7 - Strengthening the Weakest Link 26
2.5 Network Attacks - Denial of Service, Buffer Overflows, and Evasion 27
2.5.1 - DoS and DDoS Attacks 27
2.5.2 - Components of DDoS Attacks 27
2.5.3 - Mirai Botnet 29
2.5.4 - Buffer Overflow Attack 30
2.5.5 - Evasion Methods 31
2.6 SUMMARY 33

CAPITOLUL 2. NETWORK THREATS

2.0 Introduction

2.0.1 – Scope

Cine ne atacă rețeaua și de ce ? Vom afla despre diferiții actori ai amenințărilor, de asemenea, despre tehnicile și instrumentele folosite de acești „hackeri”.

2.0.2 - Obiectiv

Topic Title	Topic Objective
Who is Attacking Our Network?	Explicarea modului cum au evoluat amenințările de rețea.
Threat Actor Tools	Descrierea diferitelor tipuri de instrumente de atac utilizate de Actorii de amenințare.
Malware	Descrierea tipurilor de malware.
Common Network Attacks - Reconnaissance, Access, and Social Engineering	Explicarea atacurilor rețelelor prin metode de recunoaștere, acces și inginerie socială.
Network Attacks - Denial of Service, Buffer Overflows, and Evasion	Explicarea refuzului serviciului, depășirea tamponului și atacurile de evaziune.

2.1 Who is Attacking Our Network?

2.1.1 - Threat, Vulnerability, and Risk

Suntem atacați și atacatorii doresc acces la activele noastre. Activele sunt ceva de valoare pentru o organizație, cum ar fi datele și alte proprietăți intelectuale, servere, computere, telefoane inteligente, tablete și multe altele.

Fig. 2.1. Schema de Risk.

Pentru a înțelege mai bine orice discuție despre securitatea rețelei, este important să cunoaștem următorii termeni:

Termen	Descriere
Threat	Un pericol potențial pentru un activ, cum ar fi datele sau rețeaua în sine.
Vulnerability	O slăbiciune a unui sistem sau a designului său care ar putea fi exploatată de o amenințare.
Attack surface	O suprafață de atac este suma totală a vulnerabilităților dintr-un sistem dat care sunt accesibile unui atacator. Suprafața de atac descrie diferite puncte în care un atacator ar putea intra într-un sistem și de unde ar putea obține date din sistem. De exemplu, sistemul de operare și browserul web ar putea avea nevoie de corecții de securitate. Fiecare este vulnerabil la atacuri și este expus în rețea sau pe internet. Împreună, creează o suprafață de atac pe care actorul amenințării o poate exploata.
Exploit	Mecanismul care este utilizat pentru a valorifica o vulnerabilitate pentru a compromite un activ. Exploitările pot fi la distanță sau locale. Un exploit de la distanță este unul care funcționează în rețea fără acces prealabil la sistemul țintă. Atacatorul nu are nevoie de un cont în sistemul final pentru a exploata vulnerabilitatea. Într-un exploit local, actorul amenințării are un anumit tip de utilizator sau acces administrativ la sistemul final. O exploatare locală nu înseamnă neapărat că atacatorul are acces fizic la sistemul final.
Risk	Probabilitatea ca o anumită amenințare să exploateze o anumită vulnerabilitate a unui activ și să aibă ca rezultat o consecință nedorită.

Managementul riscului este procesul care echilibrează costurile operaționale de asigurare a măsurilor de protecție cu câștigurile obținute prin protejarea activului. Există patru moduri comune de a gestiona riscul, după cum se arată în tabel:

Risk Management Strategy	Descriere
Risk acceptance	Acesta este momentul în care costul opțiunilor de gestionare a riscului depășește costul riscului în sine. Riscul este acceptat și nu se ia nicio măsură.
Risk avoidance	Aceasta înseamnă evitarea oricărei expuneri la risc prin eliminarea activității sau dispozitivului care prezintă riscul. Prin eliminarea unei activități pentru a evita riscul, se pierd și orice beneficii posibile din activitate.
Risk reduction	Acest lucru reduce expunerea la risc sau reduce impactul riscului prin luarea de măsuri pentru a reduce riscul. Este cea mai utilizată strategie de reducere a riscurilor. Această strategie necesită o evaluare atentă a costurilor pierderii, a strategiei de atenuare și a beneficiilor obținute din operațiunea sau activitatea care este expusă riscului.
Risk transfer	O parte sau tot riscul este transferat unei terțe părți, cum ar fi o companie de asigurări.

Alți termeni de securitate a rețelei se utilizează în mod obișnuit includ:

Contramăsuri - Acțiunile care sunt luate pentru a proteja activele prin atenuarea unei amenințări sau reducerea riscului.

Impact - Daune potențiale aduse organizației care sunt cauzate de amenințare.

Notă: O exploatare locală necesită acces în interiorul rețelei, cum ar fi un utilizator cu un cont în rețea. O exploatare de la distanță nu necesită un cont în rețea pentru a exploata vulnerabilitatea acelei rețele.

2.1.2 - Hacker vs. Threat Actor

După cum știm, „hacker" este un termen comun folosit pentru a descrie un actor de amenințare. Cu toate acestea, termenul „hacker" are o varietate de semnificații, după cum urmează:

- *Un programator inteligent capabil să dezvolte noi programe și să codifice modificări la programele existente pentru a le face mai eficiente.*
- *Un profesionist în rețea care folosește abilități sofisticate de programare pentru a se asigura că rețelele nu sunt vulnerabile la atacuri.*
- *persoană care încearcă să obțină acces neautorizat la dispozitive de pe internet.*
- *persoană care rulează programe pentru a împiedica sau încetini accesul la rețea pentru un număr mare de utilizatori sau corup sau șterge datele de pe servere.*

Termenii hacker de pălărie albă, hacker de pălărie neagră și hacker de pălărie gri sunt adesea folosiți pentru a descrie hackerii.

Hackerii cu pălărie albă sunt hackeri etici care își folosesc abilitățile de programare în scopuri bune, etice și legale. Aceștia pot efectua teste de penetrare a rețelei în încercarea de a compromite rețelele și sistemele, folosind cunoștințele lor despre sistemele de securitate computerizate pentru a descoperi vulnerabilitățile rețelei. Vulnerabilitățile de securitate sunt raportate dezvoltatorilor și personalului de securitate care încearcă să repare vulnerabilitatea înainte de a putea fi exploatată. Unele organizații acordă premii sau recompense hackerilor de pălărie albă atunci când oferă informații care ajută la identificarea vulnerabilităților.

Hackerii de pălărie gri sunt persoane care comit infracțiuni și fac lucruri fără etică, dar nu pentru câștig personal sau pentru a cauza daune. Un exemplu ar fi cineva care compromite o rețea fără permisiune și apoi dezvăluie vulnerabilitatea în mod public. Hackerii grey hat pot

dezvălui o vulnerabilitate organizației afectate după ce și-au compromis rețeaua. Acest lucru permite organizației să rezolve problema.

Hackerii Black Hat sunt criminali lipsiți de etică care încalcă securitatea computerelor și a rețelei pentru câștig personal sau din motive rău intenționate, cum ar fi atacarea rețelelor. Hackerii Black Hat exploatează vulnerabilități pentru a compromite computerele și sistemele de rețea.

Bun sau rău, hacking-ul este un aspect important al securității rețelei. În acest curs, termenul de actor de amenințare este folosit atunci când se referă la acele persoane sau grupuri care ar putea fi clasificate ca hackeri de pălărie gri sau neagră.

2.1.3 - Evolution of Threat Actors

Hackingul a început în anii 1960 cu freaking-ul telefonului, sau phreaking-ul, care se referă la utilizarea diferitelor frecvențe audio pentru a manipula sistemele telefonice. În acel moment, comutatoarele telefonice foloseau diverse tonuri, sau apelarea tonurilor, pentru a indica diferite funcții. Primii actori ai amenințărilor și-au dat seama că, mimând un ton folosind un fluier, ar putea exploata comutatoarele telefonului pentru a efectua apeluri gratuite la distanță lungă.

La mijlocul anilor 1980, modemurile dial-up erau folosite pentru a conecta computerele la rețele. Actorii de amenințare au scris programe de „apelare de război” care formau fiecare număr de telefon dintr-o anumită zonă în căutarea calculatoarelor, a sistemelor de aviziere și a aparatelor de fax. Când a fost găsit un număr de telefon, au fost folosite programe de spargere a parolelor pentru a obține acces. De atunci, profilurile și motivele generale ale actorilor de amenințări s-au schimbat destul de mult.

Există multe tipuri diferite de actori ai amenințărilor.

Script kiddies au apărut în anii 1990 și se referă la adolescenți sau actori de amenințări fără experiență care rulează scenarii, instrumente și exploit-uri existente, pentru a provoca rău, dar de obicei nu pentru profit.

Vulnerability brokers - Brokerii de vulnerabilitate se referă de obicei la hackeri grey hat care încearcă să descopere exploatări și să le raporteze vânzătorilor, uneori pentru premii sau recompense.

Hacktiviștii este un termen care se referă la hackerii de pălărie gri care se adună și protestează împotriva diferitelor idei politice și sociale. Hacktiviștii protestează public

împotriva organizațiilor sau guvernelor prin postarea de articole, videoclipuri, scurgeri de informații sensibile și efectuând atacuri distribuite de refuzare a serviciului (DDoS).

Cybercriminal - Criminal cibernetic este un termen pentru hackerii de tip black hat care fie lucrează pe cont propriu, fie lucrează pentru organizații mari de criminalitate cibernetică. În fiecare an, criminalii cibernetici sunt responsabili pentru furtul de miliarde de dolari de la consumatori și companii.

State-Sponsored hackers - Hackerii sponsorizați de stat sunt actori care fură secrete guvernamentale, adună informații și sabotează rețelele guvernelor străine, ale grupurilor teroriste și ale corporațiilor. Majoritatea țărilor din lume participă într-o oarecare măsură la hacking sponsorizat de stat. În funcție de perspectiva unei persoane, aceștia sunt fie hackeri de pălărie albă, fie de pălărie neagră.

2.1.4 - Cybercriminals

Infractorii cibernetici sunt actori de amenințări care sunt motivați să facă bani folosind orice mijloace necesare. Deși uneori infractorii cibernetici lucrează independent, ei sunt mai des finanțați și sponsorizați de organizații criminale. Se estimează că la nivel global, infractorii cibernetici fură miliarde de dolari de la consumatori și companii în fiecare an.

Infractorii cibernetici operează într-o economie subterană în care cumpără, vând și comercializează exploatări și instrumente. De asemenea, cumpără și vând informațiile personale și proprietatea intelectuală pe care le fură de la victime. Criminalii cibernetici vizează întreprinderile mici și consumatorii, precum și întreprinderile și industriile mari.

2.1.5 - Cybersecurity Tasks

Actorii de amenințare nu discriminează. Acestia vizează dispozitivele finale vulnerabile ale utilizatorilor casnici și întreprinderile mici și mijlocii, precum și organizațiile mari publice și private.

Pentru a face internetul și rețelele mai sigure și mai sigure, cu toții trebuie să dezvoltăm o bună conștientizare a securității cibernetice. Securitatea cibernetică este o responsabilitate comună pe care toți utilizatorii trebuie să o practice. De exemplu, trebuie să raportăm infracțiunile cibernetice autorităților competente, să fim conștienți de potențialele amenințări din e-mail și web și să protejăm informațiile importante împotriva furtului.

Organizațiile trebuie să ia măsuri și să își protejeze activele, utilizatorii și clienții. Aceștia trebuie să dezvolte și să practice sarcini de securitate cibernetică, cum ar fi cele enumerate în figură.

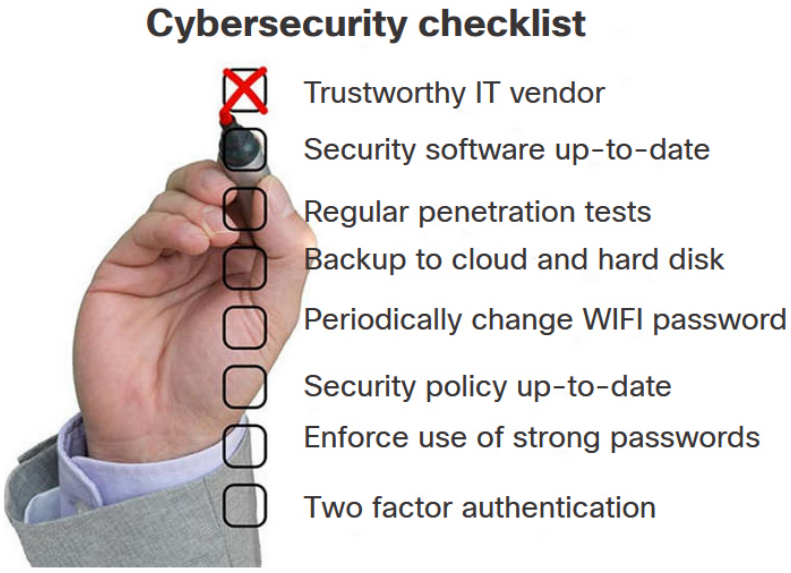


Fig. 2.2. Lista de procedure pentru protective.

2.1.6 - Cyber Threat Indicators

Multe atacuri de rețea pot fi prevenite prin partajarea informațiilor despre indicatorii de compromis (IOC). Fiecare atac are atribute identificabile unice. Indicatorii de compromis sunt dovezi că a avut loc un atac. IOC-urile pot fi caracteristici care identifică fișierele malware, adresele IP ale serverelor care sunt utilizate în atacuri, numele fișierelor și modificările caracteristice aduse software-ului sistemului final, printre altele. IOC-urile ajută personalul de securitate cibernetică să identifice ce sa întâmplat într-un atac și să dezvolte apărări împotriva atacului. Un rezumat al IOC pentru un program malware este prezentat în figură.

```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
      sha256
      6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0
      sha1    eb019ad1c73ee69195c3fc84ebf44e95c147bef8
      md5     3a104b73bb96dfed288097e9dc0a11a8
DNS requests
      domain  log.studiox.link
      domain  my.studiox.link
      domain  _sips._tcp.studiox.link
      domain  sip.studiox.link
Connections
      ip      198.51.100.248
      ip      203.0.113.82
```

De exemplu, un utilizator primește un e-mail în care susține că a câștigat un premiu mare. Făcând clic pe linkul din e-mail, rezultă un atac. IOC ar putea include faptul că utilizatorul nu a participat la acel concurs, adresa IP a expeditorului, linia de subiect al e-mailului, adresa URL pe care să da clic sau un atașament de descărcat, printre altele.

Indicatorii de atac (IOA) se concentrează mai mult pe motivația din spatele unui atac și pe posibilele mijloace prin care Actorii de amenințare au sau vor compromite vulnerabilități pentru a obține acces la active. IOA sunt preocupați de strategiile care sunt utilizate de atacatori. Din acest motiv, în loc să informeze răspunsul la o singură amenințare, IOA-urile pot ajuta la generarea unei abordări proactive de securitate. Acest lucru se datorează faptului că strategiile pot fi reutilizate în mai multe contexte și mai multe atacuri. Prin urmare, apărarea împotriva unei strategii poate preveni viitoarele atacuri care utilizează aceeași strategie sau o strategie similară.

2.1.7 - Threat Sharing and Building Cybersecurity Awareness

Guvernele promovează acum în mod activ securitatea cibernetică. De exemplu, Agenția de Infrastructură și Securitate pentru Securitate Cibernetică din SUA (CISA) conduce eforturile de a automatiza schimbul de informații de securitate cibernetică cu organizațiile publice și private fără costuri. CISA utilizează un sistem numit Automated Indicator Sharing (AIS). AIS permite partajarea indicatorilor de atac între guvernul SUA și sectorul privat de îndată ce amenințările sunt verificate. CISA oferă multe resurse care ajută la limitarea dimensiunii suprafeței de atac din Statele Unite.

CISA și Alianța Națională pentru Securitate Cibernetică (NCSA) promovează securitatea cibernetică pentru toți utilizatorii. De exemplu, au o campanie anuală în fiecare octombrie, numită „Luna națională de conștientizare a securității cibernetice” (NCASM). Această campanie a fost dezvoltată pentru a promova și a crește gradul de conștientizare cu privire la securitatea cibernetică.

Tema pentru NCASM pentru 2019 a fost „Ow IT. IT securizat. Protejați-l.” Această campanie ia încurajat pe toți cetățenii să fie mai siguri și mai responsabili personal pentru utilizarea celor mai bune practici de securitate online. Campania oferă materiale pe o mare varietate de subiecte de securitate, inclusiv:

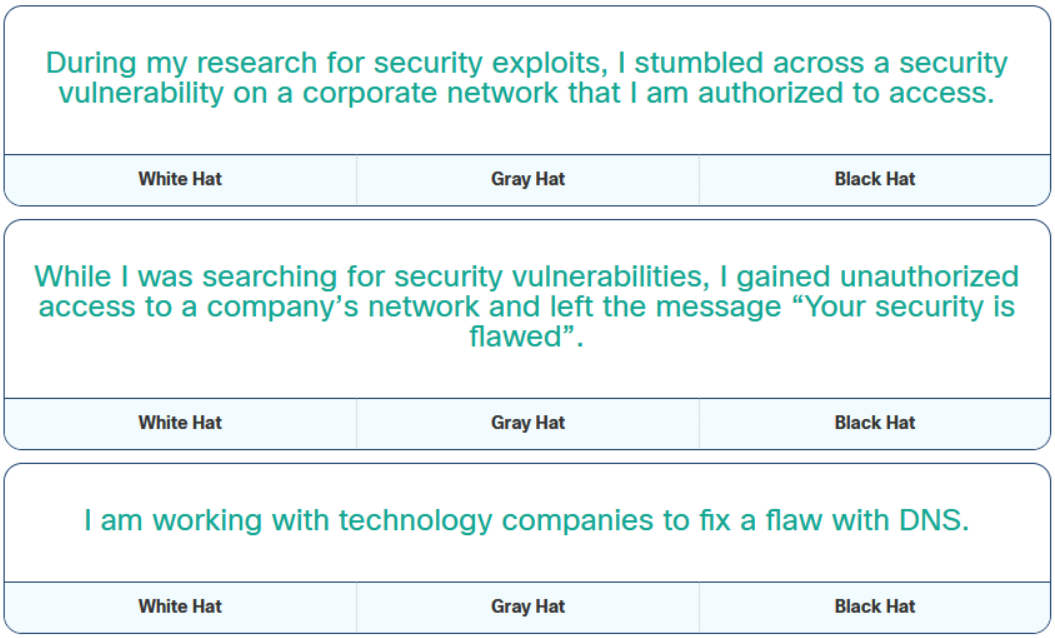
- ***Siguranța rețelelor sociale***
- ***Actualizarea setărilor de confidențialitate***

- ***Conștientizarea securității aplicației dispozitivului***
- ***Menținerea software-ului la zi***
- ***Cumpărături online sigure***
- ***Siguranță Wi-Fi***
- ***Protejarea datelor clienților***

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) oferă consiliere și soluții pentru provocările de securitate cibernetică ale statelor membre ale UE. ENISA îndeplinește un rol în Europa care este similar cu rolul CISA în SUA.

VERIFICAREA ACUMULARII CONCEPTELOR.

I hacked into ATM machines without the manufacturer's authorization and discovered several vulnerabilities. I then contacted the ATM manufacturer to share my findings with them.		
White Hat	Gray Hat	Black Hat
I secretly installed a debit card skimmer device on an ATM machine. A few days later, I retrieved it and it had captured the account numbers and pins numbers of over 1000 people. I then proceeded to transfer money from their accounts to an offshore bank account.		
White Hat	Gray Hat	Black Hat
My job is to identify weaknesses in the computer system in my company.		
White Hat	Gray Hat	Black Hat
I used malware to compromise several corporate systems to steal credit card information and sold that information to the highest bidder.		
White Hat	Gray Hat	Black Hat



2.2 Threat Actor Tools

2.2.1 - Introduction of Attack Tools

Pentru a exploata o vulnerabilitate, un actor de amenințare trebuie să aibă o tehnică sau un instrument. De-a lungul anilor, instrumentele de atac au devenit mai sofisticate și extrem de automatizate. Aceste noi instrumente necesită mai puține cunoștințe tehnice pentru a fi implementate.

În figură, se poate vedea relația dintre sofisticarea instrumentelor de atac și cunoștințele tehnice necesare pentru a le folosi.

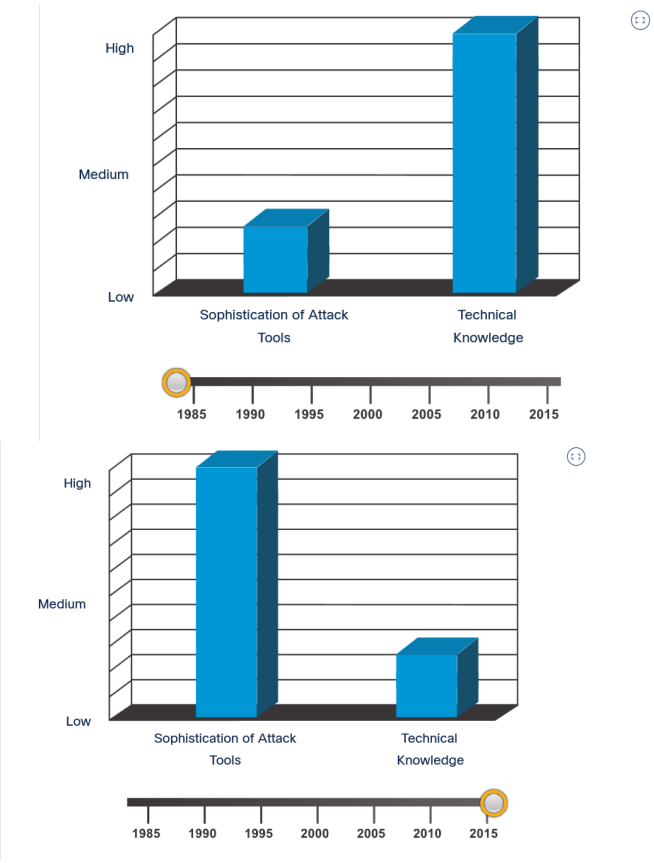


Fig. 2.3. Sofisticarea instrumentelor de atac versus cunoștințe tehnice 1985vs 2015.

2.2.2 - Evolution of Security Tools

Hackingul etic implică utilizarea multor tipuri diferite de instrumente pentru a testa rețeaua și dispozitivele finale. Pentru a valida securitatea unei rețele și a sistemelor acesteia, au fost dezvoltate multe instrumente de testare a penetrației în rețea. Cu toate acestea, multe dintre aceste instrumente pot fi utilizate și de către Actorii de amenințare pentru exploatare.

Actorii de amenințare au creat și diverse instrumente de hacking. Aceste instrumente sunt scrise în mod explicit din motive nefaste. De asemenea, personalul de securitate cibernetică trebuie să știe cum să folosească aceste instrumente atunci când efectuează teste de penetrare în rețea.

Notă: Multe dintre aceste instrumente sunt bazate pe UNIX sau Linux; prin urmare, un profesionist în securitate ar trebui să aibă un fundal puternic UNIX și Linux.

Categories of Tools	**Description**
password crackers	Parolele sunt cea mai vulnerabilă amenințare de securitate. Instrumentele de spargere a parolelor sunt adesea denumite instrumente de recuperare a parolei și pot fi folosite pentru a sparge sau recupera parola. Acest lucru se realizează fie prin eliminarea parolei originale,

	după ocolirea criptării datelor, fie prin descoperirea completă a parolei. Descoperitorii de parole fac în mod repetat presupuneri pentru a sparge parola și a accesa sistemul. Exemple de instrumente de spargere a parolelor includ John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack și Medusa.
wireless hacking tools	Rețelele wireless sunt mai susceptibile la amenințările la securitatea rețelei. Instrumentele de hacking fără fir sunt folosite pentru a sparge în mod intenționat o rețea fără fir pentru a detecta vulnerabilitățile de securitate. Exemple de instrumente de hacking wireless includ Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep și NetStumbler.
network scanning and hacking tools	Instrumentele de scanare a rețelei sunt folosite pentru a sonda dispozitivele de rețea, serverele și gazdele pentru porturi TCP sau UDP deschise. Exemple de instrumente de scanare includ Nmap, SuperScan, Angry IP Scanner și NetScanTools.
packet crafting tools	Instrumentele de creare a pachetelor sunt folosite pentru a testa și a testa robustețea unui firewall folosind pachete forjate special concepute. Exemple de astfel de instrumente includ Hping, Scapy, Socat, Yersinia, Netcat, Nping și Nemesis.
packet sniffers	Instrumentele de sniffer de pachete sunt folosite pentru a captura și analiza pachete în rețelele LAN sau WLAN tradiționale Ethernet. Instrumentele includ Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy și SSLstrip.
rootkit detectors	Un detector de rootkit este un verificator de integritate a directoarelor și fișierelor folosit de pălăriile albe pentru a detecta kiturile root instalate. Exemple de instrumente includ AIDE, Netfilter și PF: OpenBSD Packet Filter.
fuzzers to search vulnerabilities	Fuzzers sunt instrumente folosite de Actorii de amenințare atunci când încearcă să descopere vulnerabilitățile de securitate ale unui sistem informatic. Exemple de fuzzere includ Skipfish, Wapiti și W3af.
forensic tools	Hackerii cu pălărie albă folosesc instrumente criminalistice pentru a adulmeca orice urmă de dovezi existente într-un anumit sistem informatic. Exemple de instrumente includ Sleuth Kit, Helix, Maltego și Encase.
debuggers	Instrumentele de depanare sunt folosite de black hats pentru a face inginerie inversă a fișierelor binare atunci când scrieți exploit-uri. Ele sunt, de asemenea, folosite de pălăriile albe atunci când analizează programele malware. Instrumentele de depanare includ GDB, WinDbg, IDA Pro și Immunity Debugger.
hacking operating systems	Sistemele de operare de hacking sunt sisteme de operare special concepute, preîncărcate cu instrumente și tehnologii optimizate pentru hacking. Exemple de sisteme de operare special concepute pentru hacking includ Kali Linux, SELinux, Knoppix, Parrot OS și BackBox Linux.
encryption tools	Aceste instrumente protejează conținutul datelor unei organizații atunci când acestea sunt stocate sau transmise. Instrumentele de criptare folosesc scheme de algoritmi pentru a codifica datele pentru a preveni accesul neautorizat la date. Exemple de aceste instrumente includ VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN și Stunnel.
vulnerability exploitation tools	Aceste instrumente identifică dacă o gazdă la distanță este vulnerabilă la un atac de securitate. Exemple de instrumente de exploatare a vulnerabilităților includ Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit și Netsparker.
vulnerability scanners	Aceste instrumente scanează o rețea sau un sistem pentru a identifica porturile deschise. Ele pot fi, de asemenea, utilizate pentru a scana vulnerabilități cunoscute și pentru a scana mașini virtuale, dispozitive BYOD și baze de date clienți. Exemple de aceste instrumente includ Nipper, Securia PSI, Core Impact, Nessus, SAINT și Open VAS.

2.2.3 - Categories of Attacks

Actorii de amenințare pot folosi instrumentele menționate anterior sau o combinație de instrumente pentru a crea diverse atacuri. Tabelul prezintă tipuri comune de atacuri. Cu toate

acestea, lista de atacuri nu este exhaustivă, deoarece sunt descoperite în mod continuu noi modalități de a ataca rețelele.

Este important să înțelegem că actorii de amenințare folosesc o varietate de instrumente de securitate pentru a efectua aceste atacuri.

Category of Attack	Description
eavesdropping attack	Un atac de interceptare este atunci când un actor de amenințare captează și ascultă traficul din rețea. Acest atac este, de asemenea, denumit sniffing sau snooping.
data modification attack	Atacurile de modificare a datelor apar atunci când un actor de amenințare a captat traficul întreprinderii și a modificat datele din pachete fără știrea expeditorului sau destinatarului.
IP address spoofing attack	Un atac de falsificare a adresei IP este atunci când un actor de amenințare construiește un pachet IP care pare să provină de la o adresă validă în interiorul intranetului corporativ.
password-based attacks	Atacurile bazate pe parole apar atunci când un actor de amenințare obține acreditările pentru un cont de utilizator valid. Actorii amenințărilor folosesc apoi acel cont pentru a obține liste cu alți utilizatori și informații despre rețea. De asemenea, pot modifica configurațiile serverului și ale rețelei și pot modifica, redirecționa sau șterge datele.
denial-of-service (DoS) attack	Un atac DoS împiedică utilizarea normală a unui computer sau a unei rețele de către utilizatori validi. După obținerea accesului la o rețea, un atac DoS poate bloca aplicațiile sau serviciile de rețea. Un atac DoS poate inunda, de asemenea, un computer sau întreaga rețea cu trafic până când apare o oprire din cauza supraîncărcării. Un atac DoS poate bloca, de asemenea, traficul, ceea ce duce la pierderea accesului la resursele rețelei de către utilizatorii autorizați.
man-in-the-middle attack (MiTM)	Un atac MiTM are loc atunci când actorii amenințărilor s-au poziționat între o sursă și o destinație. Acum pot monitoriza, capta și controla în mod activ comunicarea în mod transparent.
compromised key attack	Un atac cu cheie compromisă are loc atunci când un actor de amenințare obține o cheie secretă. Aceasta este denumită o cheie compromisă. O cheie compromisă poate fi utilizată pentru a obține acces la o comunicare securizată fără ca expeditorul sau destinatarul să fie conștient de atac.
sniffer attack	Un sniffer este o aplicație sau un dispozitiv care poate citi, monitoriza și captura schimburile de date din rețea și poate citi pachete de rețea. Dacă pachetele nu sunt criptate, un sniffer oferă o vedere completă a datelor din interiorul pachetului. Chiar și pachetele încapsulate (tunelizate) pot fi deschise și citite dacă nu sunt criptate și actorul amenințării nu are acces la cheie.

2.3 Malware

2.3.1 - Types of Malware

Dispozitivele finale sunt în special predispuse la atacuri malware. Prin urmare, acest subiect se concentrează pe amenințările la adresa dispozitivelor finale.

Malware este prescurtarea pentru software rău intenționat sau cod rău intenționat. Este un cod sau un software conceput special pentru a deteriora, perturba, fura sau, în general, produce alte acțiuni „rele” sau ilegitime asupra datelor, gazdelor sau rețelelor.

Este important să știm despre malware, deoarece actorii amenințărilor și criminalii online încearcă frecvent să păcălească utilizatorii să instaleze malware pentru a ajuta la exploatarea lacunelor de securitate.

În plus, malware-ul se transformă atât de rapid încât incidentele de securitate legate de malware sunt extrem de frecvente, deoarece software-ul antimalware nu poate fi actualizat suficient de repede pentru a opri noile amenințări.

2.3.2 - Viruses

Un virus este un tip de malware care se răspândește prin inserarea unei copii a lui însuși într-un alt program. După rularea programului, virușii se răspândesc de la un computer la altul, infectând computerele. Majoritatea virusurilor necesită ajutor uman pentru a se răspândi. De exemplu, când cineva conectează o unitate USB infectată la computerul său, virusul va intra în computer. Virusul poate infecta apoi o nouă unitate USB și se poate răspândi pe noi computere. Virușii pot rămâne latenți pentru o perioadă lungă de timp și apoi se pot activa la o anumită oră și dată.

Un virus simplu se poate instala la prima linie de cod dintr-un fișier executabil. Când este activat, virusul poate verifica discul pentru alte executabile, astfel încât să poată infecta toate fișierele pe care încă nu le-a infectat. Virușii pot fi inofensivi, cum ar fi cei care afișează o imagine pe ecran, sau pot fi distructivi, cum ar fi cei care modifică sau șterg fișiere de pe hard disk. Virușii pot fi, de asemenea, programați pentru a muta pentru a evita detectarea.

Majoritatea virușilor sunt acum răspândiți prin unități de memorie USB, CD-uri, DVD-uri, partajări de rețea și e-mail. Virușii de e-mail sunt un tip comun de virus.

2.3.3 - Trojan Horses

Termenul de cal troian provine din mitologia greacă. Războinicii greci au oferit cadou oamenilor din Troia (troienii) un cal uriaș. Troienii au adus calul uriaș în orașul lor cu ziduri,

fără să știe că acesta conține mulți războinici greci. Noaptea, după ce majoritatea troienilor au adormit, războinicii au iesit din cal, au deschis porțile orașului și au permis unei forțe considerabile să intre și să preia orașul.

Malware-ul troian este un software care pare a fi legitim, dar conține cod rău intenționat care exploatează privilegiile utilizatorului care îl rulează, așa cum se arată în figură.

Adesea, troienii se găsesc atașați la jocurile online. Utilizatorii sunt de obicei păcăliți să încarce și să execute calul troian pe sistemele lor. În timpul jocului, utilizatorul nu va observa nicio problemă. În fundal, calul troian a fost instalat pe sistemul utilizatorului. Codul rău intenționat de la calul troian continuă să funcționeze chiar și după ce jocul a fost închis.

Conceptul de cal troian este flexibil. Poate provoca daune imediate, poate oferi acces de la distanță la sistem sau acces printr-o ușă din spate. De asemenea, poate efectua acțiuni conform instrucțiunilor de la distanță, cum ar fi „trimite-mi fișierul cu parole o dată pe săptămână”. Această tendință a malware-ului de a trimite date înapoi către criminalul cibernetic evidențiază necesitatea de a monitoriza traficul de ieșire pentru indicatorii de atac.

Caii troieni personalizați, cum ar fi cei cu o țintă specifică, sunt greu de detectat.

2.3.4 - Trojan Horse Classification

Caii troieni sunt de obicei clasificați în funcție de daunele pe care le provoacă sau de modul în care încalcă un sistem, așa cum se arată în tabel.

Type of Trojan Horse	**Description**
Remote-access	Permite accesul neautorizat de la distanță.
Data-sending	Oferă actorului amenințării date sensibile, cum ar fi parole.
Destructive	Corupe sau șterge fișiere.
Proxy	Folosește computerul victimei ca dispozitiv sursă pentru a lansa atacuri și a efectua alte activități ilegale.
FTP	Activează serviciile de transfer de fișiere neautorizate pe dispozitivele finale.
Security software disabler	Oprește funcționarea programelor antivirus sau firewall-urilor.
Denial of Service (DoS)	Încetinește sau oprește activitatea în rețea.
Keylogger	Încearcă în mod activ să fure informații confidențiale, cum ar fi numerele cardurilor de credit, prin înregistrarea tastelor introduse într-un formular web.

2.3.5 - Worms

Viermii informatici sunt similari cu virușii, deoarece se replica și pot provoca același tip de daune. Mai exact, viermii se reproduc prin exploatarea independentă a vulnerabilităților din rețele. Viermii pot încetini rețelele pe măsură ce se răspândesc de la sistem la sistem.

În timp ce un virus necesită un program gazdă pentru a rula, viermii pot rula singuri. În afară de infecția inițială, acestea nu mai necesită participarea utilizatorului. După ce o gazdă este infectată, viermele se poate răspândi foarte rapid în rețea.

Viermii sunt responsabili pentru unele dintre cele mai devastatoare atacuri de pe internet. În 2001, viermele Code Red infectase inițial 658 de servere. În 19 ore, viermele infectase peste 300.000 de servere.

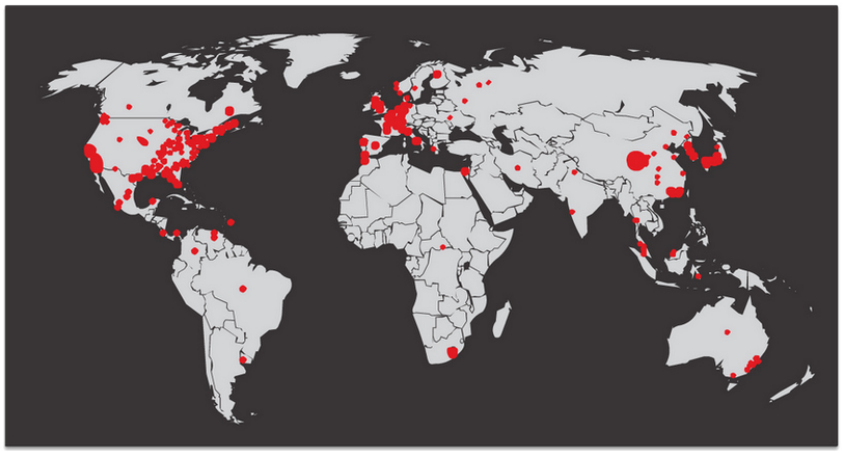


Fig. 2.4. Infectarea cu RED CODE initiala.

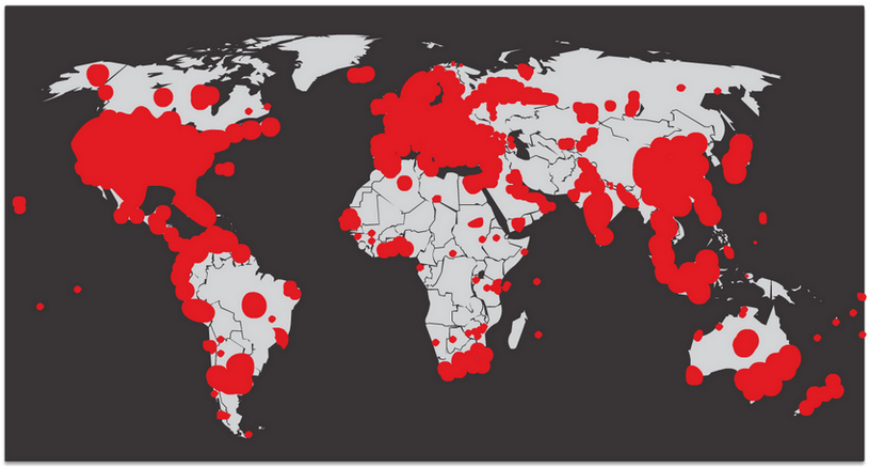


Fig. 2.5. Infectarea cu RED CODE dupa 19 ore.

Infecția inițială a viermelui SQL Slammer este cunoscută sub numele de viermele care a mâncat internetul. SQL Slammer a fost un atac de tip denial of service (DoS) care a exploatat

o eroare de depășire a tamponului în serverul SQL al Microsoft. La apogeu, numărul de servere infectate și-a dublat dimensiunea la fiecare 8,5 secunde. Acesta este motivul pentru care a reușit să infecteze peste 250.000 de gazde în 30 de minute. Când a fost lansat în weekendul din 25 ianuarie 2003, a perturbat internetul, instituțiile financiare, bancomatele și multe altele. În mod ironic, un patch pentru această vulnerabilitate fusese lansat cu 6 luni mai devreme. Serverele infectate nu aveau aplicat corecția actualizată. Acesta a fost un semnal de alarmă pentru multe organizații pentru a implementa o politică de securitate care impune ca actualizările și corecțiile să fie aplicate în timp util.

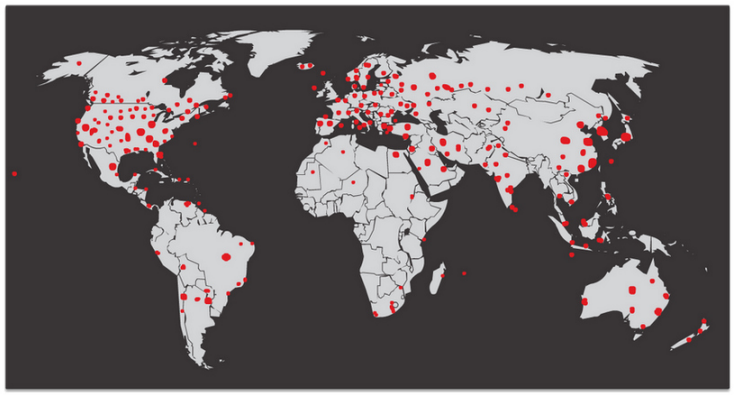


Fig. 2.7. Infectarea initiala cu SQL Slammer.

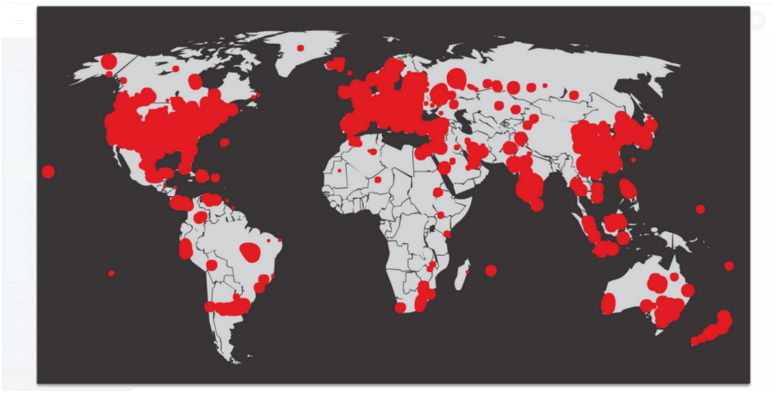


Fig. 2.8. Infectarea cu SQL Slammer dupa 30 de minute.

Viermii au caracteristici similare. Toti exploatează o vulnerabilitate gasita, au o modalitate de a se propaga și toti conțin o sarcină utilă.

2.3.6 - Worm Components

În ciuda tehnicilor de atenuare care au apărut de-a lungul anilor, viermii au continuat să evolueze și să reprezinte o amenințare persistentă. Viermii au devenit mai sofisticați în timp, dar încă tind să se bazeze pe exploatarea punctelor slabe ale aplicațiilor software.

Cele mai multe atacuri de viermi constau din trei componente, așa cum sunt enumerate în animația de mai sus.

Activarea vulnerabilității - Un vierme se instalează folosind un mecanism de exploatare, cum ar fi un atașament de e-mail, un fișier executabil sau un cal troian, pe un sistem vulnerabil.

Mecanism de propagare - După ce obține acces la un dispozitiv, viermele se reproduce și localizează noi ținte.

Payload - Sarcină utilă - Orice cod rău intenționat care are ca rezultat o anumită acțiune este o sarcină utilă. Cel mai adesea, aceasta este folosită pentru a crea o ușă din spate care permite unui actor de amenințare accesul la gazda infectată sau pentru a crea un atac DoS.

Viermii sunt programe autonome care atacă un sistem pentru a exploata o vulnerabilitate cunoscută. După exploatarea cu succes, viermele se copiază de la gazda atacatoare în sistemul nou exploatat și ciclul începe din nou. Mecanismele lor de propagare sunt de obicei implementate într-un mod greu de detectat.

Tehnica de propagare folosită de viermele Code Red este prezentată în figură.

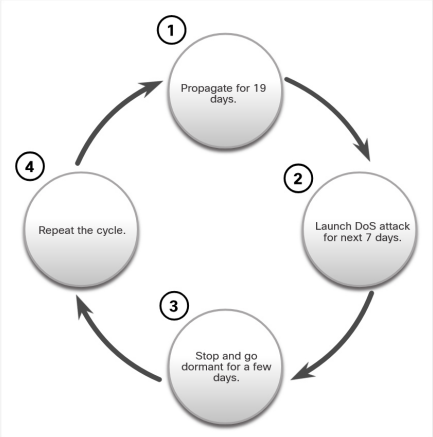


Fig. 2.8. Tehnica de propagare CODE RED.

Notă: viermii nu încetează niciodată să se răspândească pe internet. După ce sunt eliberați, viermii continuă să se propage până când toate sursele posibile de infecție sunt corectate.

2.3.7 - Ransomware

Actorii amenințărilor au folosit viruși, viermi și cai troieni pentru a-și transporta sarcinile utile și din alte motive rău intenționate. Cu toate acestea, malware-ul continuă să evolueze.

În prezent, cel mai dominant malware este ransomware. Ransomware este un malware care interzice accesul la sistemul informatic infectat sau la datele acestuia. Infractorii cibernetici cer apoi plata pentru eliberarea sistemului informatic.

Ransomware-ul a evoluat pentru a deveni cel mai profitabil tip de malware din istorie. În prima jumătate a anului 2016, campaniile de ransomware care vizau atât utilizatorii individuali, cât și utilizatorii întreprinderilor au devenit mai răspândite și mai puternice.

Există zeci de variante de ransomware. Ransomware utilizează frecvent un algoritm de criptare pentru a cripta fișierele și datele de sistem. Majoritatea algoritmilor cunoscuți de criptare a ransomware nu pot fi decriptați cu ușurință, lăsând victimelor puține opțiuni de depanare sau, "decât" să plătească prețul cerut. Plățile sunt de obicei plătite în Bitcoin, deoarece utilizatorii bitcoin pot rămâne anonimi. Bitcoin este o monedă digitală cu sursă deschisă pe care nimeni nu o deține și nu o controlează.

E-mailul și publicitatea rău intenționată, cunoscută și sub numele de malvertising, sunt vectori pentru campanii de ransomware. Ingineria socială este, de asemenea, utilizată, ca atunci când infractorii cibernetici care se identifică ca tehnicieni de securitate sună la case și îi conving pe utilizatori să se conecteze la un site web care descarcă ransomware-ul pe computerul utilizatorului.

2.3.8 - Other Malware

Acestea sunt câteva exemple de varietăți de malware moderne:

Type of Malware	Description
Spyware	Folosit pentru a colecta informații despre un utilizator și a trimite informațiile către o altă entitate fără consimțământul utilizatorului. Spyware-ul poate fi un monitor de sistem, cal troian, adware, cookie-uri de urmărire și keylogger.
Adware	Afișează ferestre pop-up enervante pentru a genera venituri pentru autorul său. Malware-ul poate analiza interesele utilizatorilor prin urmărirea site-urilor web vizitate. Apoi poate trimite reclame pop-up relevante pentru acele site-uri.
Scareware	Include software de înșelătorie care utilizează inginerie socială pentru a șoca sau a induce anxietate prin crearea percepției unei amenințări. În general, este îndreptat către un utilizator nebănuitor și încearcă să-l convingă pe utilizator să infecteze un computer, luând măsuri pentru a aborda amenințarea falsă.
Phishing	Încercările de a convinge oamenii să divulge informații sensibile. Exemplele includ primirea unui e-mail de la banca lor prin care le cere utilizatorilor să-și divulge contul și numerele PIN.
Rootkits	Instalat pe un sistem compromis. După ce este instalat, continuă să-și ascundă intruziunea și să ofere acces privilegiat actorului amenințării.

Această listă va continua să crească pe măsură ce internetul evoluează. Noi programe malware vor fi întotdeauna dezvoltate. Un obiectiv major al operațiunilor de securitate cibernetică este acela de a afla despre noile programe malware și cum să-l atenueze cu promptitudine.

2.3.9 - Common Malware Behaviors

Infractorii cibernetici modifică continuu codul malware pentru a schimba modul în care acesta se răspândește și infectează computerele. Cu toate acestea, majoritatea produc simptome similare care pot fi detectate prin monitorizarea rețelei și a jurnalului dispozitivului.

Calculatoarele infectate cu programe malware prezintă adesea unul sau mai multe dintre următoarele simptome:

- ***Apariția unor fișiere, programe sau pictograme ciudate pe desktop***
- ***Programele antivirus și firewall dezactivează sau reconfigurează setările***
- ***Ecranul computerului se blochează sau sistemul se blochează***
- ***E-mailurile sunt trimise spontan, fără știrea utilizatorului, către lista de contacte***
- ***Fișierele au fost modificate sau șterse***
- ***Creșterea utilizării CPU și/sau a memoriei***
- ***Probleme de conectare la rețele***
- ***Viteze mici ale computerului sau ale browserului web***
- ***Procese sau servicii necunoscute care rulează***
- ***Porturi TCP sau UDP necunoscute deschise***
- ***Conexiunile se fac la gazde pe Internet fără acțiunea utilizatorului***
- ***Comportament ciudat la computer***

Notă: Comportamentul programelor malware nu se limitează la lista de mai sus.

VERIFICAREA ACUMULARII CONCEPTELOR.

1. What type of malware executes arbitrary code and installs copies of itself in the memory of the infected computer? The main purpose of this malware is to automatically replicate from system to system across the network.

   - ◯ trojan horse
   - ◯ adware
   - ◯ ransomware
   - ◯ worm

2. What type of malware typically displays annoying pop-ups to generate revenue for its author?

   - ◯ adware
   - ◯ ransomware
   - ◯ scareware
   - ◯ phishing

3. What type of malware encrypts all data on a drive and demands payment in Bitcoin cryptocurrence to unencrypt the files?

   - ◯ phishing
   - ◯ scareware
   - ◯ ransomware
   - ◯ virus

4. What type of malware attempts to convince people to divulge their personally identifable information (PII)?

   - ◯ phishing
   - ◯ rootkit
   - ◯ ransomware
   - ◯ trojan horse

2.4 Common Network Attacks - Reconnaissance, Access, and Social Engineering

2.4.1 - Types of Network Attacks

Malware este un mijloc de a obține o sarcină utilă livrată. Când este livrat și instalat, sarcina utilă poate fi folosită pentru a provoca o varietate de atacuri legate de rețea din interior. Actorii amenințărilor pot ataca rețeaua și din exterior.

Există multe motive, inclusiv bani, lăcomie, răzbunare sau convingeri politice, religioase sau sociologice, pentru care actorii de amenintare ataca retelele. Profesioniștii în securitatea rețelei trebuie să înțeleagă tipurile de atacuri utilizate pentru a contracara aceste amenințări pentru a asigura securitatea rețelei LAN.

Pentru a atenua atacurile, este util să fie clasificate mai întâi diferitele tipuri de atacuri. Prin catalogarea atacurilor de rețea, este posibil să se adreseze mai degrabă tipuri de atacuri decât atacuri individuale.

Deși nu există o modalitate standardizată de clasificare a atacurilor de rețea, metoda utilizată în acest curs clasifică atacurile în trei mari categorii.

- ***Atacurile de recunoaștere***
- ***Atacurile de acces***
- ***Atacurile DoS***

2.4.2 - Reconnaissance Attacks

Recunoașterea este colectarea de informații. Este analog cu un hoț care cercetează un cartier mergând din ușă în ușă prefăcându-se că vinde ceva. Ceea ce face de fapt hoțul este să caute case vulnerabile în care să pătrundă, cum ar fi reședințe neocupate, reședințe cu uși sau ferestre ușor de deschis și acele reședințe fără sisteme de securitate sau camere de securitate.

Actorii amenințărilor folosesc atacuri de recunoaștere (sau de recunoaștere) pentru a face descoperiri neautorizate și mapare a sistemelor, serviciilor sau vulnerabilităților. Atacurile de recunoaștere preced atacurile de acces sau atacurile DoS.

Unele dintre tehnicile utilizate de actorii de amenințări rău intenționate pentru a efectua atacuri de recunoaștere sunt descrise în tabel.

Technique	Description
Perform an information query of a target	Actorul amenințării caută informații inițiale despre o țintă. Pot fi utilizate diverse instrumente, inclusiv căutarea Google, site-ul web al organizațiilor, whois și multe altele.
Initiate a ping sweep of the target network	Interogarea de informații dezvăluie de obicei adresa de rețea a țintei. Actorul amenințării poate iniția acum o verificare ping pentru a determina care adrese IP sunt active.
Initiate a port scan of active IP addresses	Acesta este folosit pentru a determina ce porturi sau servicii sunt disponibile. Exemple de scanere de porturi includ Nmap, SuperScan, Angry IP Scanner și NetScanTools.
Run vulnerability scanners	Aceasta este pentru a interoga porturile identificate pentru a determina tipul și versiunea aplicației și a sistemului de operare care rulează pe gazdă. Exemple de instrumente includ Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT și Open VAS.
Run exploitation tools	Actorul amenințării încearcă acum să descopere servicii vulnerabile care pot fi exploatate. Există o varietate de instrumente de exploatare a vulnerabilităților, inclusiv Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit și Netsparker.

2.4.3 - Access Attacks

Atacurile de acces exploatează vulnerabilitățile cunoscute în serviciile de autentificare, serviciile FTP și serviciile web. Scopul acestui tip de atac este de a obține acces la conturi web, baze de date confidențiale și alte informații sensibile.

Actorii amenințărilor folosesc atacuri de acces asupra dispozitivelor din rețea și computerelor pentru a prelua date, a obține acces sau pentru a escalada privilegiile de acces la statutul de administrator.

Atacurile cu parole - Într-un atac cu parole, actorul amenințării încearcă să descopere parole critice ale sistemului folosind diferite metode. Atacurile cu parole sunt foarte frecvente și pot fi lansate folosind o varietate de instrumente de spargere a parolelor.

Atacurile de falsificare - În atacurile de falsificare, dispozitivul actorului de amenințări încearcă să se prezinte ca un alt dispozitiv falsificând datele. Atacurile comune de falsificare includ falsificarea IP, falsificarea MAC și falsificarea DHCP.

Alte atacuri de acces includ:

- ***Exploatările de încredere***
- ***Redirecționări de porturi***
- ***Atacurile omului la mijloc***
- ***Atacurile de depășire a tamponului***

2.4.4 - Social Engineering Attacks

Ingineria socială este un atac de acces care încearcă să manipuleze indivizi pentru a efectua acțiuni sau a divulga informații confidențiale. Unele tehnici de inginerie socială sunt efectuate în persoană, în timp ce altele pot folosi telefonul sau internetul.

Ingineria sociala se bazează adesea pe dorința oamenilor de a fi de ajutor. De exemplu, un actor de amenințare ar putea suna un angajat autorizat cu o problemă urgentă care necesită acces imediat la rețea. Actorul amenințării poate face apel la vanitatea angajatului, poate invoca autoritatea folosind tehnici de scăpare a numelui sau poate face apel la lăcomia angajatului.

Informațiile despre tehnicile de inginerie socială sunt prezentate în tabel.

Social Engineering Attack	**Description**
Pretexting	Un actor de amenințare pretinde că are nevoie de date personale sau financiare pentru a confirma identitatea destinatarului.
Phishing	Un actor de amenințare trimite e-mailuri frauduloase care sunt deghizate ca provenind dintr-o sursă legitimă și de încredere pentru a păcăli destinatarul să instaleze programe malware pe dispozitivul său sau să partajeze informații personale sau financiare.
Spear phishing	Un actor de amenințare creează un atac de tip phishing, adaptat pentru o anumită persoană sau organizație.
Spam	Cunoscut și sub denumirea de e-mail nedorit, acesta este un e-mail nesolicitat care conține adesea linkuri dăunătoare, programe malware sau conținut înșelător.
Something for Something	Denumit uneori „Quid pro quo”, acesta este momentul în care un actor de amenințare solicită informații personale de la o parte în schimbul a ceva precum un cadou.
Baiting	Un actor de amenințare lasă o unitate flash infectată cu malware într-o locație publică. O victimă găsește unitatea și o introduce fără bănuială în laptopul său, instalând neintenționat malware.
Impersonation	În acest tip de atac, un actor de amenințare se preface a fi altcineva pentru a câștiga încrederea unei victime.
Tailgating	Acesta este locul în care un actor de amenințare urmează rapid o persoană autorizată într-o locație sigură pentru a obține acces la o zonă securizată.
Shoulder surfing	Un actor de amenințări se uită discret peste umărul cuiva pentru a-i fura parolele sau alte informații.
Dumpster diving	Este metoda prin care un actor de amenințări scormonește prin coșurile de gunoi pentru a descoperi documente confidențiale.

Setul de instrumente pentru ingineri sociale (SET) a fost conceput pentru a ajuta hackerii de pălărie albă și alți profesioniști în securitatea rețelelor să creeze atacuri de inginerie socială pentru a-și testa propriile rețele. Este un set de instrumente bazate pe meniu care ajută la

lansarea atacurilor de inginerie socială. SET-ul este doar în scop educațional. Este disponibil gratuit pe internet.

Întreprinderile trebuie să-și educe utilizatorii cu privire la riscurile inginerii sociale și să dezvolte strategii de validare a identităților prin telefon, prin e-mail sau în persoană.

Figura arată practicile recomandate care ar trebui urmate de toți utilizatorii.

Fig. 2.9. Practici recomandate de protecție a ingineriei sociale

2.4.7 - Strengthening the Weakest Link

Securitatea cibernetică este la fel de puternică ca veriga sa cea mai slabă. Deoarece computerele și alte dispozitive conectate la internet au devenit o parte esențială a vieții noastre, ele nu mai par noi sau diferite.

Oamenii au devenit foarte dezinvolti în utilizarea acestor dispozitive și rareori se gândesc la securitatea rețelei. Cea mai slabă verigă în securitatea cibernetică poate fi personalul din cadrul unei organizații, iar ingineria socială o amenințare majoră pentru securitate.

Din acest motiv, una dintre cele mai eficiente măsuri de securitate pe care le poate lua o organizație este să își instruiască personalul și să creeze o „cultură conștientă de securitate”.

2.5 Network Attacks - Denial of Service, Buffer Overflows, and Evasion

2.5.1 - DoS and DDoS Attacks

Un atac de tip Denial of Service (DoS) creează un fel de întrerupere a serviciilor de rețea pentru utilizatori, dispozitive sau aplicații. Există două tipuri majore de atacuri DoS:

Cantitate copleșitoare de trafic - actorul amenințării trimite o cantitate enormă de date la o rată pe care rețeaua, gazda sau aplicația nu o pot gestiona. Acest lucru face ca timpii de transmisie și de răspuns să încetinească. De asemenea, poate bloca un dispozitiv sau un serviciu.

Pachete formatate rău intenționat - actorul amenințării trimite un pachet formatat rău intenționat către o gazdă sau o aplicație, iar receptorul nu este în măsură să-l gestioneze. Acest lucru face ca dispozitivul de recepție să funcționeze foarte lent sau să se blocheze.

Atacurile DoS reprezintă un risc major deoarece întrerup comunicarea și provoacă pierderi semnificative de timp și bani. Aceste atacuri sunt relativ simplu de efectuat, chiar și de către un actor necalificat.

Un atac DoS distribuit (DDoS) este similar cu un atac DoS, dar provine din mai multe surse coordonate. De exemplu, Un actor de amenințare construiește o rețea de gazde infectate, cunoscută sub numele de zombi. Actorul amenințării folosește un sistem de comandă și control (CnC) pentru a trimite mesaje de control zombi. Zombii scanează și infectează în mod constant mai multe gazde cu malware bot. Malware-ul bot este conceput pentru a infecta o gazdă, făcându-l un zombi care poate comunica cu sistemul CnC. Colecția de zombi se numește botnet. Când este gata, actorul amenințării instruiește sistemul CnC să determine rețeaua botnet de zombi să efectueze un atac DDoS.

2.5.2 - Components of DDoS Attacks

Dacă actorii amenințărilor pot compromite multe gazde, ei pot efectua un atac DoS distribuit (DDoS). Atacurile DDoS sunt similare ca intenție cu atacurile DoS, cu excepția faptului că un atac DDoS crește în amploare deoarece provine din surse multiple coordonate, așa cum se arată în figură. Un atac DDoS poate folosi sute sau mii de surse, ca în atacurile DDoS bazate pe IoT.

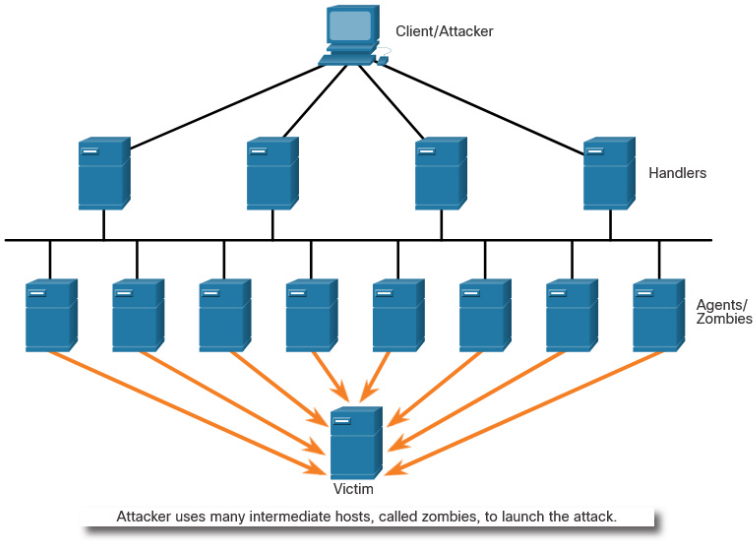


Fig. 2.10. Atac de tip DDoS.

Următorii termeni sunt se utilizează pentru a descrie componentele unui atac DDoS:

Component	Description
zombies	Aceasta se referă la un grup de gazde compromise (adică agents). Aceste gazde rulează cod rău intenționat denumit roboți (adică bots). Malware-ul zombi încearcă continuu să se autopropage ca un vierme.
bots	Boții sunt programe malware care sunt concepute pentru a infecta o gazdă și pentru a comunica cu un sistem de gestionare. Boții pot, de asemenea, să înregistreze apăsările de la taste, să adune parole, să captureze și să analizeze pachete și multe altele.
botnet	Aceasta se referă la un grup de zombi care au fost infectați cu ajutorul programelor malware cu autopropagare (adică, roboți) și sunt controlați de manageri.
handlers	Aceasta se referă la un server primar de comandă și control (command-and-control CnC sau C2) care controlează grupuri de zombi. Creatorul unei rețele bot poate folosi Internet Relay Chat (IRC) sau un server web pe serverul C2 pentru a controla de la distanță zombii.web server on the C2 server to remotely control the zombies.
botmaster	Acesta este actorul amenințării care deține controlul asupra rețelei botnet și asupra gestionarilor.

Notă: Există o economie subterană în care botnet-urile pot fi cumpărate (și vândute) pentru o taxă nominală. Acest lucru poate oferi actorilor de amenințări rețele bot ale gazdelor infectate gata să lanseze un atac DDoS împotriva țintei alese.

2.5.3 - Mirai Botnet

Mirai este un program malware care vizează dispozitivele Internet of Things (IoT) care sunt configurate cu informații de conectare implicite. Camerele de televiziune cu circuit închis (CCTV) au reprezentat majoritatea țintelor lui Mirai. Folosind un atac de dicționar de forță brută, Mirai a trecut printr-o listă de nume de utilizator și parole implicite care erau larg cunoscute pe internet.

- ***root/implicit***
- ***rădăcină/1111***
- ***root/54321***
- ***admin/admin1234***
- ***admin1/parolă***
- ***oaspete/12345***
- ***tehnologie/tehnică***
- ***sprijin/sprijin***

După ce a obținut accesul cu succes, Mirai a vizat utilitățile BusyBox bazate pe Linux care rulează pe aceste dispozitive. Aceste utilitare au fost folosite pentru a transforma dispozitivele în roboți care puteau fi controlați de la distanță ca parte a unei rețele bot. Rețeaua botnet a fost apoi utilizată ca parte a unui atac distribuit de refuz de serviciu (DDoS). În septembrie 2016, un botnet Mirai de peste 152.000 de camere CCTV și video recordere digitale (DVR) a fost responsabil pentru cel mai mare atac DDoS cunoscut până la acel moment. Cu un trafic de vârf de peste 1 Tb/s, a eliminat serviciile de găzduire ale unei companii de găzduire web din Franța.

În octombrie 2016, serviciile Dyn, un furnizor de servicii de nume de domeniu (DNS), au fost atacate, provocând întreruperi de internet pentru milioane de utilizatori din Statele Unite și Europa.

Notă: În decembrie 2017, trei actori americani de amenințări au pledat vinovați că au conspirat pentru „a desfășura atacuri DDoS împotriva site-urilor web și a companiilor de găzduire web situate în Statele Unite și în străinătate”. Cei trei infractori riscă până la 10 ani de închisoare și amenzi de 250.000 de dolari.

2.5.4 - Buffer Overflow Attack

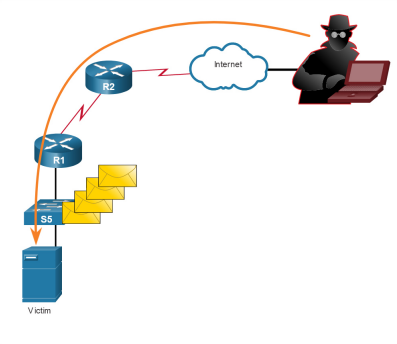


Fig. 2.11. Atac de tip Buffer Overflow.

Scopul unui actor de amenințare atunci când folosește un atac DoS de depășire a tamponului este de a găsi o defecțiune legată de memoria sistemului pe un server și de a o exploata. Exploatarea memoriei tampon prin copleșirea acesteia cu valori neașteptate face de obicei sistemul inoperabil, creând un atac DoS.

De exemplu, un actor de amenințare introduce o intrare care este mai mare decât se aștepta de către aplicația care rulează pe un server. Aplicația acceptă cantitatea mare de intrare și o stochează în memorie. Rezultatul este că poate consuma memoria tampon asociată și poate suprascrie memoria adiacentă, corupând eventual sistemul și provocând blocarea acestuia.

Un exemplu timpuriu de utilizare a pachetelor malformate a fost Ping of Death. În acest atac moștenit, actorul amenințării a trimis un ping de moarte, care a fost o cerere de ecou într-un pachet IP mai mare decât dimensiunea maximă a pachetului de 65.535 de octeți. Gazda care primește nu ar putea gestiona un pachet de această dimensiune și s-ar prăbuși.

Atacurile de depășire a tamponului evoluează continuu. De exemplu, o vulnerabilitate de atac de refuz de serviciu la distanță a fost descoperită recent în Microsoft Windows 10. Mai exact, un actor de amenințări a creat cod rău intenționat pentru a accesa memoria în afara domeniului de aplicare. Când acest cod este accesat de procesul Windows AHCACHE.SYS, încearcă să declanșeze o blocare a sistemului, interzicând serviciul utilizatorului. Pe internet pe „blogul TALOS-2016-0191” pentru a accesa site-ul web de informații despre amenințări Cisco Talos și pentru a citi o descriere a unui astfel de atac.

Notă: Se estimează că o treime din atacurile rău intenționate sunt rezultatul depășirilor de buffer.

2.5.5 - Evasion Methods

Actorii de amenințări au învățat cu mult timp în urmă că „a ascunde înseamnă a prospera”. Aceasta înseamnă că programele lor malware și metodele de atac sunt cele mai eficiente atunci când sunt nedetectate. Din acest motiv, multe atacuri folosesc tehnici de evaziune ascunse pentru a masca o sarcină utilă de atac. Scopul lor este de a preveni detectarea evitând apărarea rețelei și a gazdei.

Unele dintre metodele de evaziune folosite de actorii amenințărilor includ:

Evasion Method	**Description**
Encryption and tunneling	Această tehnică de evaziune folosește tunelul pentru a ascunde sau criptarea pentru a amesteca fișierele malware. Acest lucru face dificil pentru multe tehnici de detectare a securității să detecteze și să identifice malware-ul. Tunnelarea poate însemna ascunderea datelor furate în interiorul pachetelor legitime.
Resource exhaustion	Această tehnică de evaziune face gazda țintă prea ocupată pentru a utiliza în mod corespunzător tehnicile de detectare a securității.
Traffic fragmentation	Această tehnică de evaziune împarte o sarcină utilă rău intenționată în pachete mai mici pentru a ocoli detectarea securității rețelei. După ce pachetele fragmentate ocolesc sistemul de detectare a securității, malware-ul este reasamblat și poate începe să trimită date sensibile din rețea.
Protocol-level misinterpretation	Această tehnică de evaziune apare atunci când apărarea rețelei nu gestionează în mod corespunzător caracteristicile unei PDU, cum ar fi o sumă de control sau o valoare TTL. Acest lucru poate păcăli un firewall să ignore pachetele pe care ar trebui să le verifice.
Traffic substitution	În această tehnică de evaziune, actorul amenințării încearcă să păcălească un IPS, ofuscând datele din sarcina utilă. Acest lucru se face prin codificarea într-un format diferit. De exemplu, actorul amenințării ar putea folosi traficul codificat în Unicode în loc de ASCII. IPS nu recunoaște adevărata semnificație a datelor, dar sistemul final țintă poate citi datele.
Traffic insertion	Similar cu înlocuirea traficului, dar actorul amenințării inserează octeți suplimentari de date într-o secvență rău intenționată de date. Regulile IPS ratează datele rău intenționate, acceptând întreaga secvență de date.
Pivoting	Această tehnică presupune că actorul amenințării a compromis o gazdă din interior și dorește să-și extindă accesul mai mult în rețeaua compromisă. Un exemplu este un actor de amenințare care a obținut acces la parola de administrator pe o gazdă compromisă și încearcă să se conecteze la o altă gazdă folosind aceleași acreditări.
Rootkits	Un rootkit este un instrument complex pentru atacatori, folosit de actori cu experiență în amenințări. Se integrează cu cele mai joase niveluri ale sistemului de operare. Când un program încearcă să listeze fișiere, procese sau conexiuni la rețea, rootkit-ul prezintă o versiune igienizată a rezultatului, eliminând orice ieșire incriminatoare. Scopul rootkit-ului este de a ascunde complet activitățile atacatorului pe sistemul local.
Proxies	Traficul din rețea poate fi redirecționat prin sisteme intermediare pentru a ascunde destinația finală pentru datele furate. În acest fel, comanda-și-controlul cunoscut nu poate fi blocat, deoarece destinația proxy-ului pare benignă. În plus, în cazul în care datele sunt furate, destinația datelor furate poate fi distribuită între mai mulți proxy, fără a atrage atenția asupra faptului că o singură destinație necunoscută servește drept destinație pentru cantități mari de trafic de rețea.

Noi metode de atac sunt în curs de dezvoltare. Personalul de securitate al rețelei trebuie să cunoască cele mai recente metode de atac pentru a le detecta.

1. What is the weakest link in network security?

- ◯ reconnaissance
- ◯ access
- ◯ DoS
- ◯ social engineering

2. What type of attack is tailgating?

- ◯ reconnaissance
- ◯ access
- ◯ DoS
- ◯ social engineering

3. What type of attack is port scanning?

- ◯ reconnaissance
- ◯ access
- ◯ DoS
- ◯ social engineering

4. What is the weakest link in network security?

- ◯ routers
- ◯ people
- ◯ TCP/IP
- ◯ social engineering

2.6 SUMMARY

Cine ne atacă rețeaua?

Înțelegerea securității rețelei necesită să înțelegeți următorii termeni: amenințare, vulnerabilitate, suprafață de atac, exploatare și risc. Managementul riscului este procesul care echilibrează costurile operaționale de asigurare a măsurilor de protecție cu câștigurile obținute prin protejarea activului. Patru moduri comune de a gestiona riscul sunt acceptarea riscului, evitarea riscului, reducerea riscului și transferul riscului. Hacker este un termen folosit pentru a descrie un actor de amenințare. Hackerii cu pălărie albă sunt hackeri etici care își folosesc abilitățile în scopuri bune, etice și legale. Hackerii de pălărie gri sunt persoane care comit infracțiuni și fac lucruri lipsite de etică, dar nu pentru câștig personal sau pentru a cauza pagube. Hackerii Black Hat sunt criminali care încalcă securitatea computerelor și a rețelei pentru câștig personal sau din motive rău intenționate, cum ar fi atacarea rețelelor. Actorii de amenințări includ copii de scenarii, brokeri de vulnerabilitate, hacktiviști, criminali cibernetici și hackeri sponsorizați de stat. Multe atacuri de rețea pot fi prevenite prin partajarea informațiilor despre IOC. Multe guverne promovează securitatea cibernetică. CISA și NCSA sunt exemple de astfel de organizații.

Introducerea instrumentelor de atac

Actorii de amenințări folosesc o tehnică sau un instrument. Instrumentele de atac au devenit mai sofisticate și extrem de automatizate. Multe dintre instrumente sunt bazate pe Linux sau UNIX și cunoașterea acestora este utilă unui profesionist în securitate cibernetică. Instrumentele includ instrumente de spargere a parolelor, instrumente de hacking fără fir, instrumente de scanare și hacking pentru securitatea rețelei, instrumente de fabricare a pachetelor, instrumente de fabricare a pachetelor, instrumente de sniffer de pachete, detectoare de rootkit, instrumente de căutare a vulnerabilităților, instrumente criminalistice, depanare, sisteme de operare de hacking, instrumente de criptare, instrumente de exploatare a vulnerabilităților. , și scanere de vulnerabilități. Categoriile de atacuri includ atacuri de interceptare, atacuri de modificare a datelor, atacuri de falsificare a adresei IP, atacuri bazate pe parole, atacuri de refuzare a serviciului, atacuri de tip man-in the middle, atacuri cu cheie compromisă și atacuri sniffer.

Programe malware

Malware este prescurtarea pentru software rău intenționat sau cod rău intenționat. Actorii amenințărilor încearcă frecvent să păcălească utilizatorii să instaleze programe malware pentru a ajuta la exploatarea vulnerabilităților dispozitivelor finale. Adesea, software-ul antimalware nu poate fi actualizat suficient de rapid pentru a opri noile amenințări. Trei tipuri comune sunt virusul, viermele și calul troian. Un virus este un tip de malware care se răspândește prin inserarea unei copii a lui însuși într-un alt program. Majoritatea virușilor sunt răspândiți prin unități de memorie USB, CD-uri, DVD-uri, partajări de rețea și e-mail. Malware-ul troian este un software care pare a fi legitim, dar conține cod rău intenționat care exploatează privilegiile utilizatorului care îl rulează. Adesea, troienii se găsesc pe jocurile online. Caii troieni sunt de obicei clasificați în funcție de pagubele pe care le provoacă. Tipurile de cai troieni includ acces la distanță, trimitere de date, distructiv, proxy, FTP, dezactivare software de securitate, DoS și keylogger. Viermii sunt asemănători cu virușii, deoarece se replic și pot provoca același tip de daune. Virușii necesită un program gazdă pentru a rula. Viermii pot alerga singuri. Majoritatea atacurilor de viermi constau din trei componente: vulnerabilitatea de activare, mecanismul de propagare și sarcina utilă. În prezent, ransomware-ul este cel mai dominant malware. Acesta interzice accesul la sistemul infectat sau la datele acestuia. Infractorii cibernetici cer apoi plata pentru eliberarea sistemului informatic. Alte exemple de programe malware includ spyware, adware, scareware, phishing și rootkit-uri.

Atacurile comune de rețea – recunoaștere, acces și inginerie socială

Actorii amenințărilor pot ataca rețeaua și din exterior. Pentru a atenua atacurile, este util să clasificați diferitele tipuri de atacuri. Cele trei categorii majore sunt atacurile de recunoaștere, acces și DoS. Recunoașterea este colectarea de informații. Actorii amenințărilor fac descoperiri și cartografiere neautorizate a sistemelor, serviciilor sau vulnerabilităților. Atacurile Recon preced accesul sau atacurile DoS. Unele dintre tehnicile utilizate includ următoarele: efectuarea unei interogări de informații despre o țintă, inițierea unei verificări ping a rețelei țintă, inițierea unei scanări de porturi a adreselor IP active, rularea scanerelor de vulnerabilitate și rularea instrumentelor de exploatare. Atacurile de acces exploatează vulnerabilitățile cunoscute în serviciile de autentificare, serviciile FTP și serviciile web. Aceste atacuri includ atacuri de parole, atacuri de falsificare, atacuri de exploatare a încrederii, redirecționări de porturi, atacuri de tip man-in-the-middle și atacuri de depășire a memoriei tampon. Ingineria socială este un atac de acces care încearcă să manipuleze indivizi pentru a

efectua acțiuni nesigure sau a divulga informații confidențiale. Aceste atacuri includ pretexte, phishing, spear phishing, spam, ceva pentru ceva, momeală, uzurparea identității, tailgating, surfing la umăr și scufundări în tomberon.

Atacurile de rețea – refuzarea serviciului, depășiri de buffer și evaziune

Atacurile DoS creează un fel de întrerupere a serviciilor de rețea pentru utilizatori, dispozitive sau aplicații. Există două tipuri majore: cantitate copleșitoare de trafic și pachete formatate rău intenționat. Atacurile DDoS sunt similare ca intenție cu atacurile DoS, cu excepția faptului că