හැක් කිරීමේ ආචාරධර්ම සහ තොරතුරු තාක්ෂණය භාවිතාවේ ආරක්ෂාව

Easy way to learn Ethical Hacking & IT Security

ඩී.පී. සෙනරත් යාපා

කර්තෘ ප්‍රකාශනයකි

පෙරවදන

තොරතුරු තාක්ෂණය භාවිතාවේ ආරක්ෂාව සහ හැක් කිරීමේ ආචාරධර්ම අද පරිගණකය ක්ෂේත්‍රයේ නියැලී සිටින සියලුම තරා තිරම් වන බාල වැඩිහිටි මහළු වයස් කාණ්ඩ වලට අයත් පරිශීලකයන් අනිවාර්යයෙන්ම දැනගත යුතු වටිනා කෘතියකි. සිය අධ්‍යාපනය ලබන වයසේ දරුවන් අතරද මෙම හැක් කිරීමේ විෂය දැනටම ඉතාමත් ජනප්‍රිය වී ඇතී එමෙන්ම වර්තමානයේදී සහ අනාගතයේදී ඕනෑම කාර්යයක යෙදීමට හෝ විෂයක් ඉගෙනීමට ඇති ප්‍රධානතම මාධ්‍යය පරිගණකය වන නිසා එය භාවිතයේදී ඉතාමත් තදින්ම අවශ්‍යය වන ආරක්ෂාව පිළිබඳ දැනුම අනිවාර්යයෙන්ම දරුවනට ලබාදීම දෙමාපියන් වන අප කාගේත් යුතුකමකි.

එයට ප්‍රධන හේතුව නම් අද අපට දිනපතා අසන්නට දකින්නට ලැබෙන ඇතැම් සිද්ධීන් නිසා මෙහි ඇති අයහපත් පැත්ත පිළිබඳ දරුවන්ට සහ තරුණ තරුණියන්ට හට ඒ පිළිබඳ නිසි අවබෝධයක් නොමැති බවය. විශේෂයෙන් පාසල් යන වයසේ දරු දැරියන්ට සහ පරිගණක විෂය පිළිබඳ ඇල්මක් ඇති පිරිසට තොරතුරු තාක්ෂණය භාවිතයේදී ඇතිවන අවදානම පිළිබඳවත් තොරතුරු තාක්ෂණය ආරක්ෂාකාරී ලෙස භාවිත කරන්නේ කෙසේද යන්නත් කිසියම් ගැටලුවක් පැනනැගුණු විට ගතයුතු ක්‍රියාමාර්ග පිළිබඳවත් මා මෙම පොතෙහි මනාව පැහැදිලි කර දී ඇති සියලුම දෙනා මෙම පොත නිසි අවබෝධ යෙන් කියවීමෙන් තොරතුරු තාක්ෂණය භාවිතයේදී ඇතිවන අවධානම් තත්ත්වයන් බොහෝ දුරට තේරුම් ගෙන තාක්ෂණය ආරක්ෂාකාරී ලෙස භාවිතා කිරීමට මාර්ගෝපදේශකත්වය ලැබේවා යැයි මා ගේ ප්‍රාර්ථනාවයි.

ඩී.පී. සෙනරත් යාපා
PGDip (UK), NDT (Electronics), MCP, MOS, ECDL(UK)
0772953717, 0715901737
නො.04, අරලිය උයන
මැදකන්ද පාර, මත්තෙගොඩ
2017 **ජූලි මස** 29 **වැනිදා ය.**

මෙම පොතෙහි අඩංගු කරුණු

1

ජාලකරණයේ අත්‍යවශ්‍යාංග (Network Essentials)

2

හැකර් (hacker) යනු කුමක්ද ?

3

මෙම විනිවිදුම් පරීක්ෂාව (Penetration Testing)

4

Microsoft Windows Attacks හඳුනා ගනිමු

5

Linux Exploitation හදුනා ගනිමු

6

Wireless Hacking හැඳින්වීම

7

විද්‍යුත් තැපැල් පණිවිඩ (E-mail) Hacking

8

Facebook හැකර් යනු කවුරුන්ද?

9

ශ්‍රී ලංකාව සිදු වන Cyber crimes

10

ලොව පුරා සිදු වන සයිබර් ප්‍රහාර (Global Cyber-attacks)

1

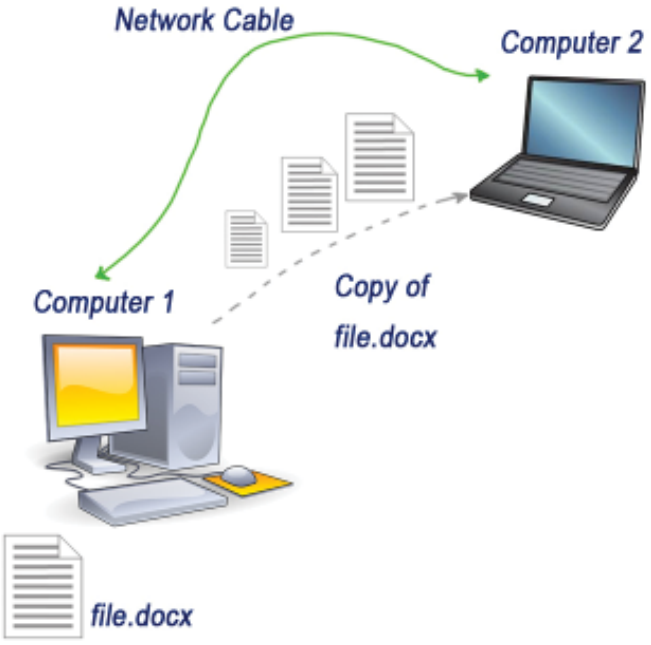
ජාලකරණයේ අත්‍යවශ්‍යාංග (Network Essentials)

ජාලකරණය හඳුන්වා දීම (Introduction to Networking)

ජාලකරණය යනු, අවම වශයෙන් පරිගණක දෙකක් හෝ ඊට වැඩි ගණනක්, හෝ වෙනත් ඉලෙක්ට්‍රෝනික උපකරණයක් එකිනෙකට සම්බන්ධ කිරීම මගින් ඒ එකිනෙක හරහා දත්ත හුවමාරු කර ගැනීමය.

උදාහරණයක් ලෙස පරිගණක දෙකක් අතර ඇති ලිපිගොනු Share කර ගැනීමට ජාලකරණය මගින් සිදු කළ හැකි අතර (share files), පරිශ්‍රීලකයන් අතර පණිවුඩ (users to message each other) හුවමාරු කර ගත හැකිය. තවද ජාලකරණය සිදුවී තිබෙන ප්‍රදේශය තුල සම්භන්ධ කර පවතින මුද්‍රණ යන්ත්‍ර share කර ගත හැකිය (share a single printer).

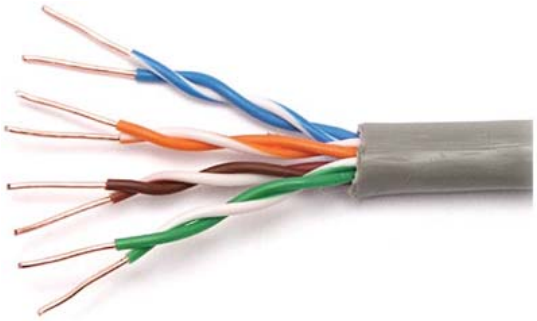
ජාලකරණයේදී පරිගණක අතර සම්බන්ධතාවය (Network connection) පවත්වා ගැනීම සඳහා පහත පරිදි නියමානුකූලව cables (වයර්) භාවිතයට ගන්නා නමුත් මෙම ජාල අතර සම්බන්ධතා ඇති කර ගැනීමට රේඩියෝ සංඥා radio signals (wireless / wi-fi), දුරකථන මාර්ග telephone lines හෝ ඉතා දුරින් පවතින satellite ජාල ද මේ සඳහා භාවිතයට ගනු ලබයි.



පරිගණක දෙකක් අතර ලිපිගොනුවක් ජාලකරණයේ සිදුවන අවස්ථාව

භෞතික මාධ්‍යන් ඔස්සේ දත්ත සම්ප්‍රේෂණය

භෞතික මාධ්‍යන් ඔස්සේ දත්ත සම්ප්‍රේෂණයේදී අතීතයේ සිට කොඇක්ෂියල් රැහැන් (Coaxial Cable) භාවිතයට ගන්නා ලද අතර තාක්ෂණයේ දියුණුවත් සමග අද ලෝකයේ සහ ශ්‍රී ලංකාව තුල බහුලවම භාවිතා වන කේබල් වර්ගයය නම් යුගල රැහැන් (Twisted Pair Wire) වර්ගයයි. පහත පරිදි යුගල රැහැන් නිර්මාණය වී තිබෙනුයේ පරිවාරක වලින් ආවරණය වූ සන්නායක තන්තු 2 ක් එකිනෙක එතීමෙන් තැණුන යුගල තන්තු කිහිපයක් නැවත වතාවක් පොදුවේ තවත් පරිවාරක කොටසකින් ආවරණය වීමෙනි.



මෙම කේබල් වර්ග අනුව Data Speed අගයන් වෙනස් වනු ඇත.

කේබල් වර්ග	වේගය	තාක්ෂණික නාමය
Catergory 1	1Mbps	Voice Only
Catergory 3	10Mbps	10BaseT Ethernet
Catergory 5	100Mbps	100BaseT Ethernet
Catergory 5E	100Mbps (2 pair)	Gigabit Ethernet
Catergory 6	1000Mbps	Gigabit Ethernet

ෆයිබර් ඔප්ටික් (ප්‍රකාශ තන්තු) Fiber Optic

මෙම රැහැන් ඉතා සිහින් ආරක්ෂක ස්තරයකින් ආවරණය කරන ලද (silicon) වීදුරු සූත්‍රිකා වලින් සමන්විත වේ. ගමන් කරන්නේ සිහින් ආලෝක ධාරාවකි. මෙමගින් ආලෝකය ඉතා දිගු දුරකට, විහිදුවන හෙයින් ඉතා ඉහල දත්ත පරාසයක් ඉතා දිගු දුරකට සම්ප්‍රේෂණය කිරීමට හැකියාව පවති. දිගු දුර Cabling සඳහා යොදාගැනීමට දැනට ලෝකයේ ඇති හොඳම රැහැන් වර්ගය මෙයයි. මෙම ඈෂ්ටික තන්තු විද්‍යුත් චුම්භක විකිරණ මගින් විකෘත නොවීම මෙහි ඇති විශේෂ ලක්ෂණයයි. සම්ප්‍රේෂණ වේගය තත්පරයට බිටු ට්‍රිලියනයකට වඩා ඉහළ අගයක් ගනු ලබයි.

	Optical Fiber	Copper
දුර ප්‍රමාණය	40Km	100m
දුරට අනුව වේගය	10,000 Mbps	1000 Mbps
උපරිම කලාපය	69Tbps	10Gbps

ජාලකරණය අපට ඇයි අවශ්‍යය (Why Use Networks?)

- පරිගණක භාවිතා කරමින් ජාලකරණයේ යෙදීමට ඉඩදීම මගින්.
- පහසුවෙන් දත්ත සහ ලිපිගොනු (files and data) share කර ගත හැකිවේ.
- හවුලේ සම්පත් භාවිතය (share resources) ලෙස. අන්තර්ජාලය සහ මුද්‍රණ යන්ත්‍ර එක් කිරීමේ හැකියාව.
- වෙනත් ජාලයන් වල සිටින පරිශ්‍රීලකයන් සමග සන්නිවේදනය සිදුකල හැකිවීම (ඊමේල්, ක්ෂණික කෙටි ඇමතුම් instant messaging, විද්‍යුත්මාධ්‍ය සාකච්ඡා (video conferencing).
- File server භාවිතා කරගනිමින් පහසුවෙන් දත්ත ගබඩා කර ගැනීම සහ ඒවා පහසුවෙන් access කර හැකි වීම.
- ජාලය අධීක්ෂණය හා පාලනය කිරීම (Traffic monitoring and control) වැනි කළමනාකරණ සේවා සඳහා.

මෙම ජාලකරණය කරන ලද පරිගණක අපි අන්තර්ජාලයට සම්බන්ධ කළහොත් අපට පහත සියලුම වැඩසටහන් ජාලගත පරිගණක තුලින් ප්‍රවේශය විය හැකිය.

- ඊ-වාණිජ්‍යය වැනි අන්තර්ජාල සේවාවන් භාවිතා කර බැංකු කටයුතු සිදුකළ හැකි වීම.
- පර්යේෂණ සඳහා විශාල පරාසයක තොරතුරු වෙත පිවිසීමට හැකි වීම.
- විනෝදාස්වාද ක්‍රීඩා වලි යෙදීමට හැකිවීම.
- සමාජ ජාලා වෙබ් අඩවි ෆෙස්බුක්, LinkdIn, Twitter වැනි වැඩසටහන් සමග සම්බන්ධවීමට හැකිවීම.

ජාලකරණය භාවිතයට නොගැන සිටීමට හේතු

ජාලයකට සම්බන්ධ වූ පරිගණකයක් භාවිතා නොකර සිටීමට බලපාන හේතු කිහිපයක් පහත පරීදි පෙන්වා දිය හැකිවේ.

- පරිගණකය හැකර් ප්‍රහාරයකට ගොදුරු වීම.
- ජාලය බිඳ වැටුණහොත්, බොහෝ කාර්යයන් සිදුකර ගැනීම ඉතා අසීරු වීම.
- ඔබේ පරිගණකයට පහසුවෙන් වෛරසයක් පහර දිය හැකි වීම.

විශේෂයෙන්ම, අපි අන්තර්ජාලයට සම්බන්ධ පරිගණකයක් භාවිතා කරනවා නම් පහත කරුණු පිළිබඳව අවධානයෙන් සිටින්න.

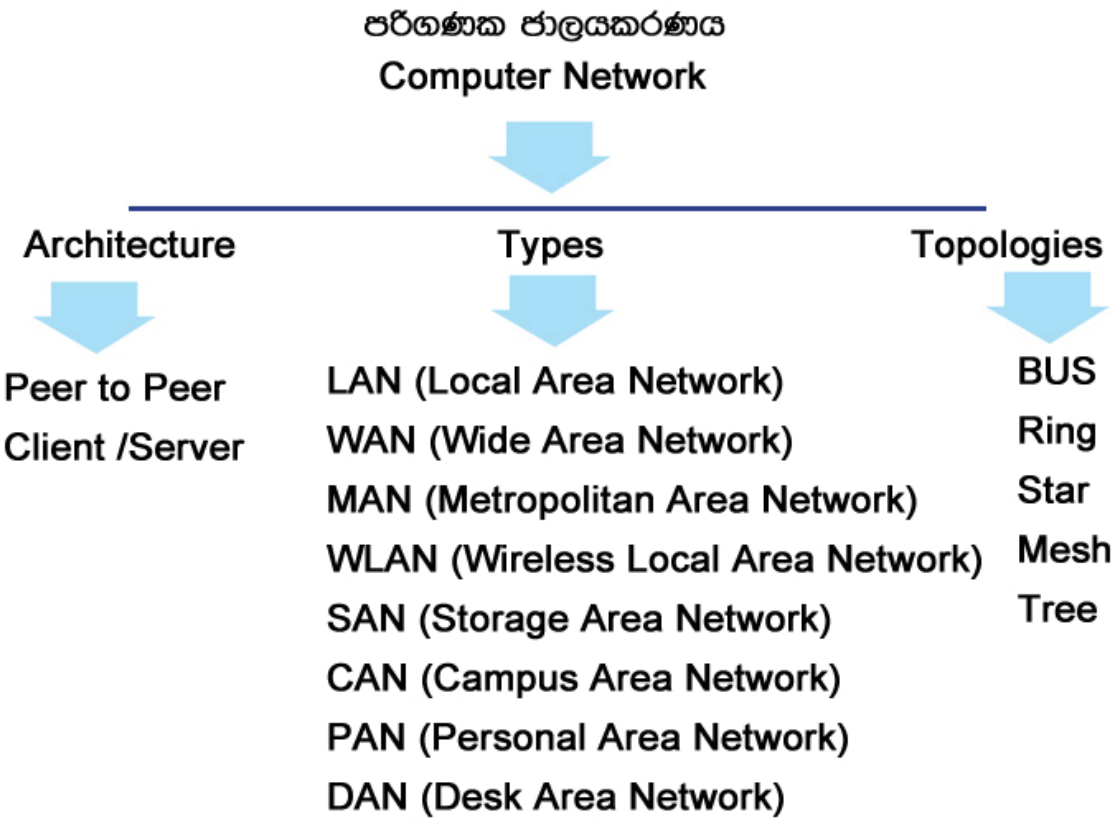
- අපගේ පුද්ගලික තොරතුරු හෙළි කිරීම සම්බන්ධයෙන් අප පරෙස්සම් විය යුතුය.
- Malware මෘදුකාංග අඩංගු විය හැකි සැක සහිත වෙබ් අඩවි භාවිතයෙන් වැළකී සිටින්න.
- අන්තර්ජාලය ඔස්සේ සොයාගත් තොරතුරු සෑම විටම නිවැරදි හෝ විශ්වසනීය නොවන බව අප දැන සිටින්න.

ජාලකරණය නිසා සේවාදායට ලැබෙන සේවාවන්,

ජාලකරණය intranet හෝ Internet සේවාවක් ලෙස පරිශීලකයින්ට ප්‍රවේශය වීමට ඉඩ සලසා ඇත. ජාලකරණ සේවාදායකයන් විසින් සපයන සේවාවන් කිහිපයක් පහත දක්වා තිබේ.

ලිපි ගොනු හුවමාරු කිරීමේ සේවය (File Transfer)
World Wide Web සේවය (WWW)
විද්‍යුත් තැපෑල් සේවය (E-mail)

පරිගණක ජාලයකරණය (Computer Networking)



ඉහත පරිගණක පරිගණක ජාලයකරණයට අනුව ජාල ආකෘති (Network Architechtures) වර්ග දෙකකින් සමන්විත වේ. එය පහත අයුරින් ඔබට පැහැදිලි කර දිය හැකිවේ.

1. Peer to Peer ආකෘතිය (Workgroup)

මෙහිදී පරිගණකයක දෙකක් ජාලගත කරන අයුරු රූප සටහනින් පෙන්වා දී ඇත.

crossover patch cable භාවිතයට ගනිමින් පරිගණකයක දෙකක් ඒවායේ network adapters දෙක crossover වර්ගයේ කේබලයක් මගින් එකිනෙක ජාලගත කළ හැකිවේ.

පරිගණකයක දෙකක් හෝ ඊට වැඩි ප්‍රමාණයක් ජාලගතකරණ සිදු වන අයුරු අපි දැන් සලකා බලමු.

මෙහිදී network hub හෝ switch භාවිතයට ගනිමින් පරිගණක දෙකක් හෝ ඊට වැඩි ප්‍රමාණයක් ජාලයට සම්බන්ධ කිරීම සිදුකල හැකිය.

2. Client/ Server ආකෘතිය (Domain)

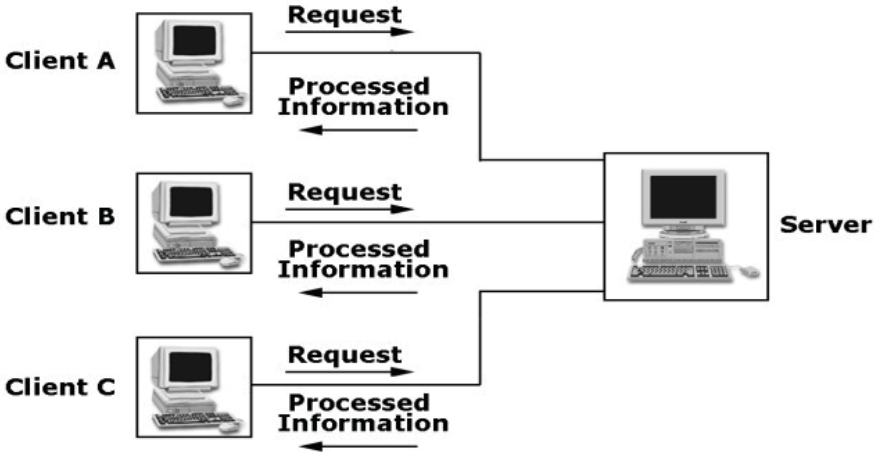
ජාලයක් නිර්මාණය කිරීම සඳහා පරිගණකය Client (workstation) සහ Server ලෙස වර්ග දෙකකකින් ක්‍රියා කරනු ලබයි.

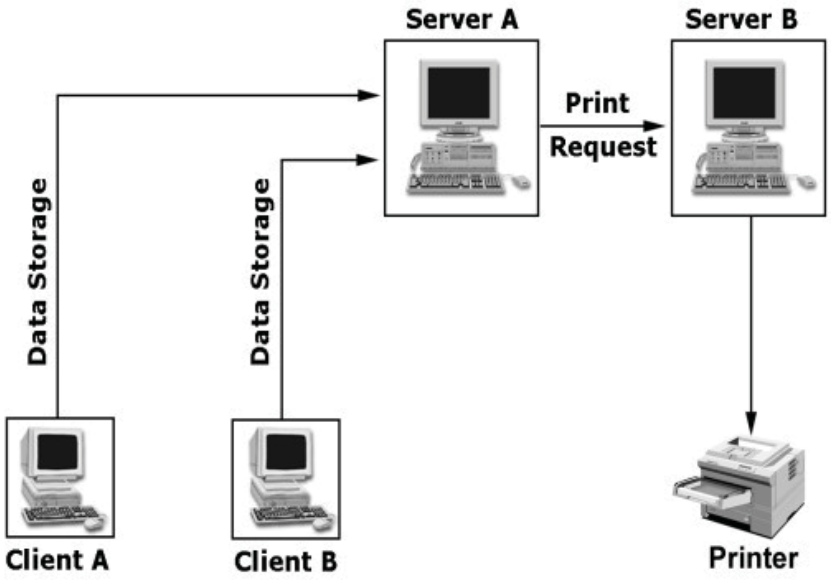
Client නැතහොත් workstations පරිගණක් එදිනෙදා අපගේ කාර්යයන් ඉටු කිරීම සඳහා භාවිතයට ගනු ලබන සාමාන්‍යය පරිගණකයයි නමුත්, Server යනු ජාලයේ Client පරිගණක සඳහා “සේවා” සපයන විශේෂ බලවත් පරිගණක් වේ.

ප්‍රධාන සේවාව වර්ග කිහිපයක්,

- මධ්‍යගත ස්ථානයක සිට පොදු ලිපිගොනු ගබඩා කිරීම.
- මුද්‍රණ යන්ත්‍ර වැනි උපාංග Share කර ගැනීම.
- ජාලයට පිවිසීමට හෝ පිවිසිය නොහැකි වීමට හැකි ලෙස එය පාලනය කිරීම.
- අන්තර්ජාල සම්බන්ධතාවය Share කිරීම.

Client/ Server ආකෘතිය පිළිබඳ පහත රූපසටහන් හරහා තවදුරටත් සළකා බලමු.





Client/ Server ජාලයට අදාල මෙම රූපසටහන් සලකා බැලීමේ දී Client A, B සහ C යන පරිගණක Server සමග සම්බන්ධ වන අයුරු සහ Server A සහ B යන පරිගණක Client A, B සමගත් මුද්‍රණ යන්ත්‍රය සමගත් සම්බන්ධ වන අයරු ඉහත පෙන්වා දී තිබේ.

රැහැන්ගත (wired) ජාල භාවිතයේ ඇති වාසි

ස්ථාපිත පිරිවැය සලකා බැලීමේදී Ethernet කේබල්ස්, hubs සහ switches මිළදී ගැනීමට ඔබට විශාල වියදමක් නොවිය හැකි නමුත් කේබල් ජාල ගත කිරීමේදී යම් අධික මුදලක් වැය කිරීමට සිදුවනු ඇත.

රැහැන්ගත තාක්ෂණය අතිශයින් විශ්වාසදායී වන අතර Ethernet කේබල් හා hubs වැනි උපාංග සෑම විටම වැඩි දියුණු වී වෙළඳපොළට පැමිනෙන අතර ජාලය තුල බොහෝ දුරට නොසැලකිලිමත් සම්බන්ධතාවයක් සිදුවන්නේ නම් එය loose cable හෝ improper connection මත සිදුවනු ඇත.

කාර්ය සාධනය අතින් ඔබට වඩාත් වේගවත් ලිපිගොනු හුවමාරුව සහ අධිවේගී අන්තර්ජාල ප්‍රවේශය (internet broadband) සඳහා රැහැන්ගත තාක්ෂණය උපයෝගී කර ගනු ලැබේ. මෙම රැහැන් ජාල රැහැන් රහිත ජාලයන්ට සාපේක්ෂව සන්නිවේදනය අතින් සුරක්ෂිතය.

රහිත (wireless) ජාල භාවිතයේ ඇති වාසි

මෙම ජාල භාවිතයේ දී ඔබට මේ සඳහා අවශ්‍යය වන්නේ පරිගණක Wireless Adapter උපාංග යයි. රැහැන් රහිත ජාලය ආවරණය කිරීමේදී ඔබේ ලැප්ටොප් පරිගණකය ඕනෑම ස්ථානයකට රැගෙන යා හැකි අතර එමගින් වඩා හොඳ සංචලනය පහසු කරයි. රැහැන් රහිත router වල මිල අඩුවීම නිසා රැහැන් රහිත ජාලය භාවිත කරන නිවාස සංඛ්‍යාව වර්තමානයේ වැඩිවෙමින් තිබේ.

	Wired	Wireless
ස්ථාපනය (Installation)	මධ්‍යයස්ථ අපහසුතාවයක්	පහසු වන නමුත් මැදිහත්වීම් අතර සිදු වේ
පිරිවැය (Cost)	අඩු අගයකි	වැඩි පුර අවශ්‍ය වේ
විශ්වසනීයත්වය (Reliability)	අධිකය	සාධාරණ ඉහල අගයකි
කාර්ය සාධනය (Perfomance)	බොහොම හොඳයි	සාධාරණ අගයකි
ආරක්ෂාව (Securtiy)	සාධාරණ අගයකි	සාධාරණ අගයකි
ජංගමතාව (Mobility)	සීමා සහිතය	සතුටුදායකයි

802.11 රැහැන් රහිත තාක්ෂණයේ ප්‍රමිතීන් (Wireless standards)

IEEE 802.11 යනු 900 MHz සහ 2, 4, 3, 6, 5, සහ 60 GHz සංඛ්‍යාත කලාප වල පවතින රැහැන් රහිත (WLAN) ප්‍රාදේශීය ජාලයන් හදුන්වා දෙනු ලබන ප්‍රමිතීන්ය. මෙහි දී පරිගණක සන්නිවේදනය ස්ථාපනය කිරීම සඳහා media access control (MAC) සහ භෞතික ස්ථරය (PHY) භාවිතා පරනු ලබයි. එම නිර්මාණය කාර්යය සිදු කිරීම විද්‍යුත් හා ඉලෙක්ට්‍රොනික ඉංජිනේරු ආයතනය (IEEE) සහ LAN/ MAN සම්මත කමිටුව (IEEE 802) විසින් පවත්වා ගෙන යනු ලැබේ. එසේම පහත පරිදි 802.11 රැහැන් රහිත තාක්ෂණයේ (wireless technology) ක්‍රියාකාරිත්වය දැඩි ලෙස රඳා පවතින්නේ පරිගණකය හා access point හෝ wireless router අතර දුර ප්‍රමාණය මතය.

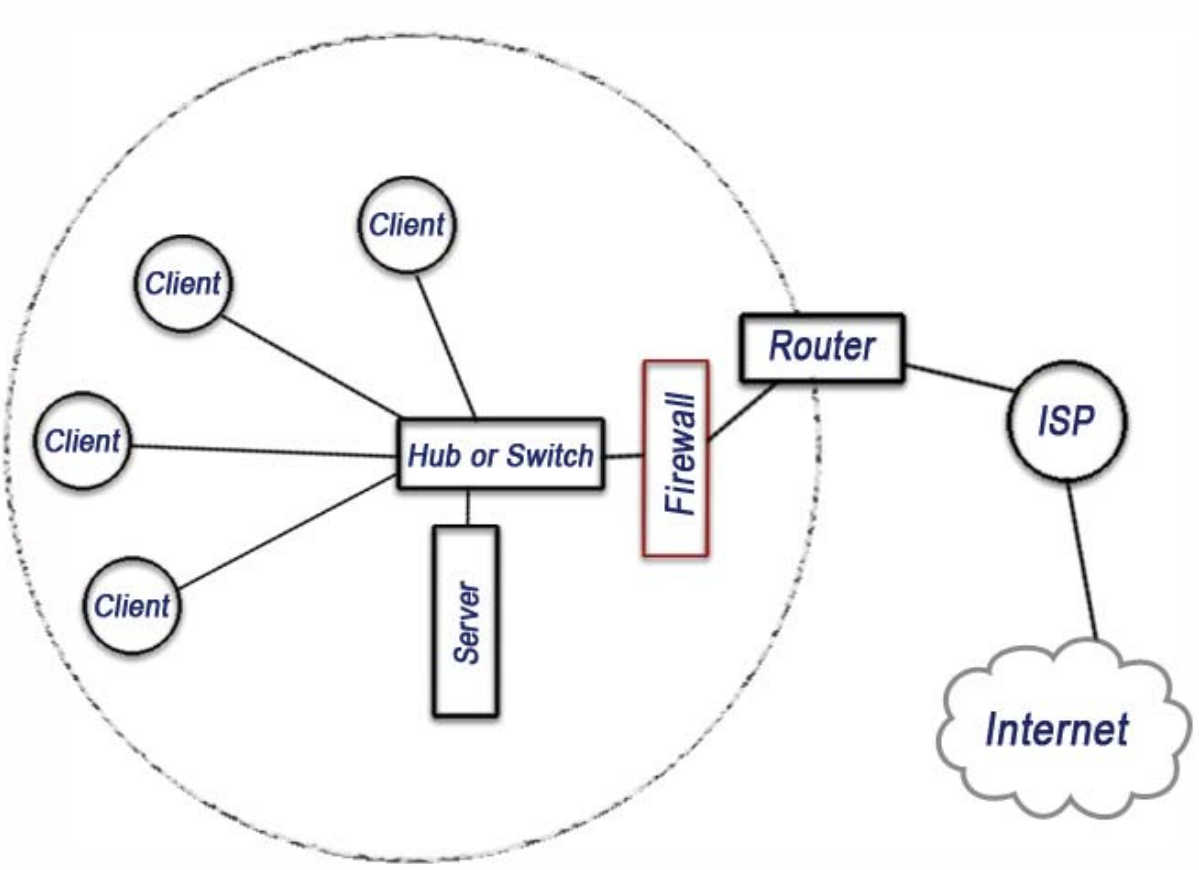
IEEE ප්‍රමිතීන්	වර්ෂය	සංඛ්‍යාතය	උපරිම වේගය	ගෘහස්ථ පරාසය	විළිමහන් පරාසය
802.11a	1999	5 GHz	54 Mbps	30 m	120 m
802.11b	1999	2.4 GHz	11 Mbps	30 m	135 m
802.11g	2003	2.4 GHz	54 Mbps	40 m	135 m
802.11n	2009	2.4/5 GHz	600 Mbps	70 m	250 m
802.11ac	2014	5 GHz	1 Gbps	30 m	300 m

ආරක්ෂාව අවදානමට ලක්වීම රැහැන් රහිත සංඥා වාතයේ ගමන් කරන අතර Wired Equivalent Privacy (WEP) භාවිතා කරමින් ජාලය මගින් සංකේතාත්මක ආකාරයෙන් දත්ත යැවීමෙන් තොරව හැකර් මගින් අවහිර කළ හැකිවේ.

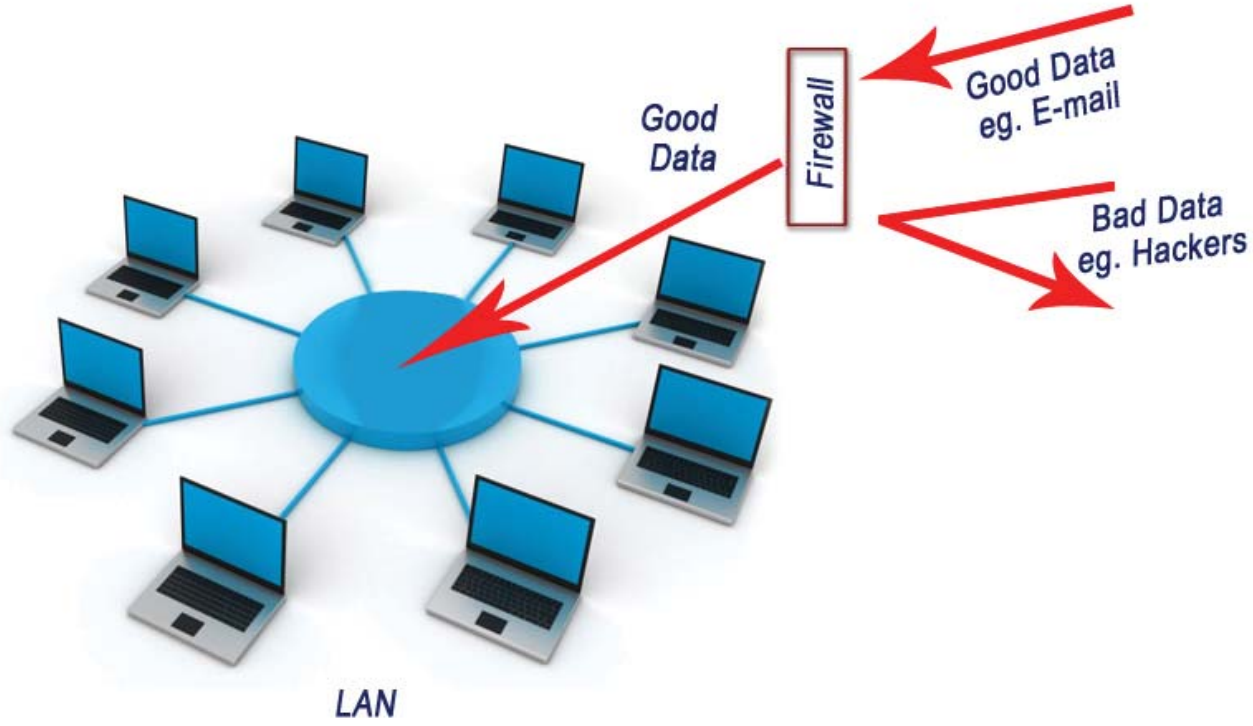
ආරක්ෂාව සඳහා නිසි අවධානයක් යොමු කළ හැකිනම් රැහැන් රහිත ජාලයන් බොහෝ නිවෙස් සහ කාර්යාල වලට ගැලපෙන පහසුම ජාල ක්‍රමයකි.

Firewall

Firewall යනු ඉලෙක්ට්‍රෝනික උපාංගයකි. එය ඔබගේ පරිගණකය හා සෙසු ජාලය අතර සන්නිවේදනයේ ආරක්ෂාකාරීත්වය පවත්වා ගෙන යාමට භාවිතා කරන මෘදුකාංගයකි.
ඔබගේ LAN ජාලය hacker ප්‍රහාරයන් ගෙන් ආරක්ෂා කර ගැනීමට ඔබ කැමති නම්, LAN සහ අන්තර්ජාල සම්බන්ධතාව අතරට Firewall උපාංගය ඔබ විසින් ස්ථාපනය කිරීම සිදුකල යුතුවේ.



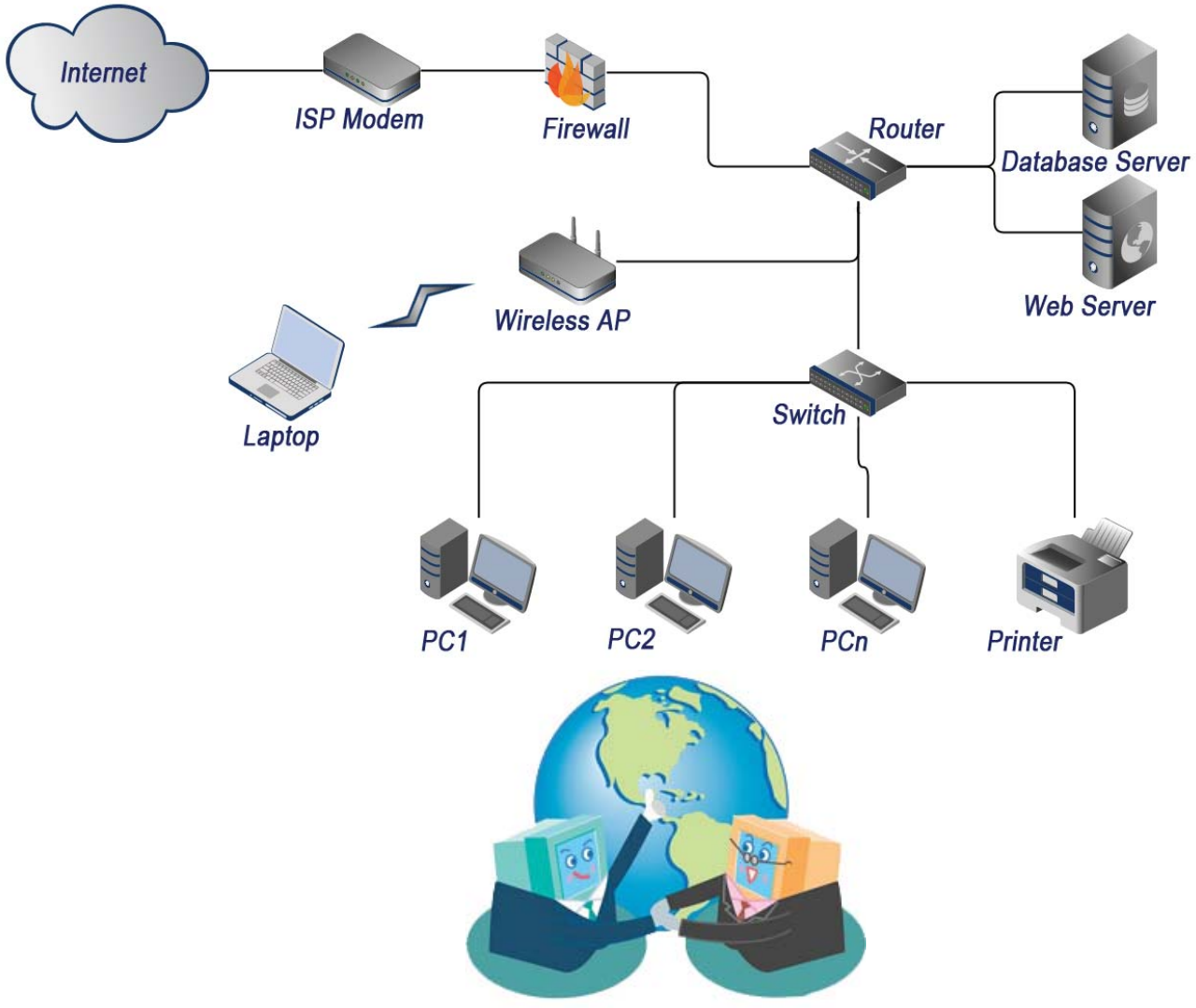
Firewall මගින් ඔබේ පරිගණකය හෝ LAN වෙත පැමිණීමට වෙර දරන අනවසර සම්බන්ධතා අවහිර කරන (blocks unauthorised connection) අතර සාමාන්‍යය දත්ත උදාහරණ ලෙස ඊ-මේල් හෝ වෙබ් පිටු ඇතුල් වීමට පහත පරිදි ඉඩ ලබා දෙනු ලැබේ.



කුඩා ප්‍රමාණයක ජාලයක් සාදාගනිමු (Setting Up a Small Network)

ඔබට කුඩා ලෙස ජාලයක් සාදා ගැනීමට අවශ්‍යය නම් එය සිදුකර ගැනීමට පහත දෘඩකාංග භාවිතා කළ යුතුවේ.

- එකකට හෝ ඊට වැඩි switches හෝ hubs එකට සම්බන්ධ කිරීම.
- switches වෙත උපාංගය සම්බන්ධ කිරීම සඳහා ජාල කේබල්.
- වෙනම රැහැන් රහිත පිවිසුමක්, (wireless access point) wireless උපාංග සම්බන්ධ කිරීමට. (උදා: ලැප්ටොප් හෝ ස්මාර්ට් ජංගම දුරකථන)
- router උපාංගයක් LAN සිට Internet (WAN) සම්බන්ධ කිරීම.
- ඔබේ ජාලය හැකර් සිට ආරක්ෂා කිරීම සඳහා firewall උපාංගයක්.
- Bridge උපාංගය ඔබට තවත් නව ජාලය වෙත සම්බන්ධ වීමට අවශ්‍යය නම්.
- Server එකක් හෝ කීපයක ජාල ගොනු ගබඩා කිරීමට.
- මුද්‍රණ යන්ත්‍ර වැනි shared resource වැනි ජාල ක්‍රියාකාරකම් සම්බන්ධ කිරීම.



දත්ත ආරක්ෂාව (Data Security)

ඔබේ පරිගණකය, ජාලයට සම්බන්ධ කළ වහාම ඔබගේ ලිපිගොනු සහ තොරතුරු ආදී දත්තයන්ගේ සුරක්ෂිතභාවය ගැන සිතන්න පටන් ගත යුතුය.

ජාලයක් මගින් පුද්ගලයකුට ඔබගේ පරිගණකයට physicaly ප්‍රවේශ වීමට ඉඩ සලසනු ලබන නිසා (ඔවුන් ඔබ ඉදිරියෙහි නොසිට) මෙමගින් එම පුද්ගලයා හට ඔබගේ පරිගණකයේ සියළුම ස්ථානවලට ප්‍රවේශ විය හැකිය. පරිගණක පද්ධතියකට අනවසරයෙන් ප්‍රවේශය ලබා ගන්නා පුද්ගලයකු බොහෝ විට hacker ලෙස හැඳින්වේ.

අනවසර ප්‍රවේශය වැළැක්වීම (Preventing Unauthorised Access)

ඔබගේ පරිගණකය හැකර් වෙත ප්‍රවේශ වීම වැළැක්වීම සඳහා ගත හැකි ආරක්ෂිත ක්‍රම ගණනාවක් ඇති අතර ඉන් කිහිපයක් පහත පෙන්වා දී ඇත.

භෞතික ආරක්ෂාව

පළමු කරුණ ලෙස තහවුරු කර ගැනීමට අවශ්‍යය වනුයේ ඔබගේ ජාලයේ ඇති පරිගණක තුලට අනවසර පුද්ගලයින්ට ඇතුල්වීමට (physically access) ඉඩ ලබා නොදිය යුතුය. විශේෂයෙන්ම එය ඉදිරියෙහි වාඩිවී ඒවා පරිහරණ කිරීමට ඉඩ නොදිය යුතුය. උදාහරණයක් වශයෙන්, කාර්යාල වල Server room වල දොරවල් අගුලු දැමීමෙන් පරිශීලක නාම (Username) සහ හොඳ මුරපද (Password) යෙදීම සිදු කල යුතුයි.

ඔබගේ පරිගණකයේ දත්ත ආරක්ෂා කිරීම සඳහා වඩාත් පොදු ක්‍රමයක් වනුයේ පරිශීලක ගිණුම් සහ මුරපද භාවිතා කිරීමය. මෙහිදී පරිශීලක නාමයක් නැති අයෙකු හෝ නිවැරදි මුරපදය නොදන්නා අයෙකුට ජාලය තුලට ප්‍රවේශ වීම අහිමි වනු ඇත.

මෙය සාර්ථක වීම සඳහා පහසුවෙන් guess කර ජාලය තුලට ප්‍රවේශ වීමට යොදා ගන්නා මුරපදයක් නොවිය යුතුය. මුරපදය අහඹු ලෙස තෝරා ගනු ලබන lowercase letters, uppercase letters and numbers වලින් සමන්විය යුතුවේ. සංකේත (symbols) යොදා ගත හැකි නම් ඔබගේ එම මුරපදය තවත් ශක්තිමත් වනු ඇත.

දුර්වල මුරපද - password, 123456, david, 27dec2002
ශක්තිමත් මුරපද - s63gRdd1, G66ew$dQ, gdr298783X

සමහර පරිගණක පද්ධති මගින් පරිශීලක නාම සහ මුරපදය වෙනුවට ඔවුන්ගේ හැඳුනුම්පත scanne කිරීම, ඇඟිලි සලකුණු පාඨකයන් ලබා ගැනීම, voice හෝ print recognition ආදිය ආදේශ කර ගනු ලබයි.

Encrypt ක්‍රමය හරහා දත්ත ආරක්ෂා කිරීම

අපට බොහෝ විට පුද්ගලික හෝ රහසිගත තොරතුරු තිබේ. අනවසර පුද්ගලයින් විසින් මෙම දත්ත බැලීමෙන් ආරක්ෂා කර ගත යුතුය. අන්තර්ජාලය වැනි පොදු ජාලයක් හරහා දත්ත යැවිය යුතු නම් මෙම දත්ත විශේෂයෙන් ආරක්ෂාකාරීව යැවිය යුතුවේ.

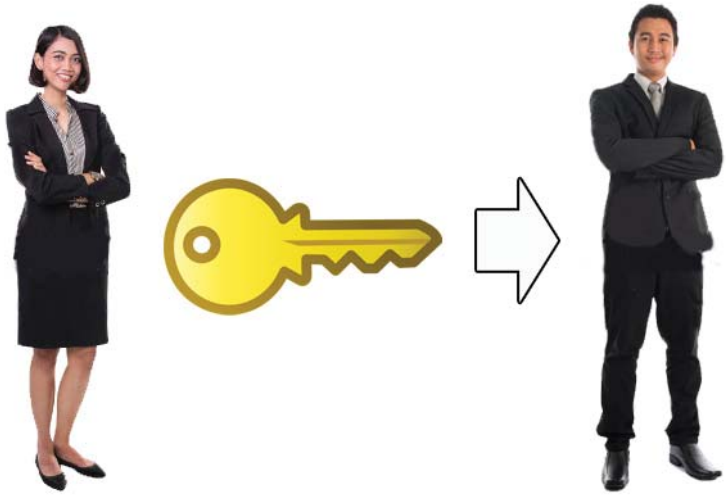
මේ සඳහා හොඳම ආරක්ෂක ක්‍රමය නම් ඒවා ගුප්තකේතනය නැති නම් encrypt කිරීමයි. දත්ත ගුප්තකේතනය (Data Encryption) සිදු කරන අයුරු පහත පරීදි සළකා බලමු.

ගුප්තකේතන Key, හිමිකරුවන් හැර අන් කිසිවෙකුට අර්ථවත් නොවන ආකාරයේ තොරතුරු පරිවර්තනය කිරීමේ ක්‍රියාවලියයි.

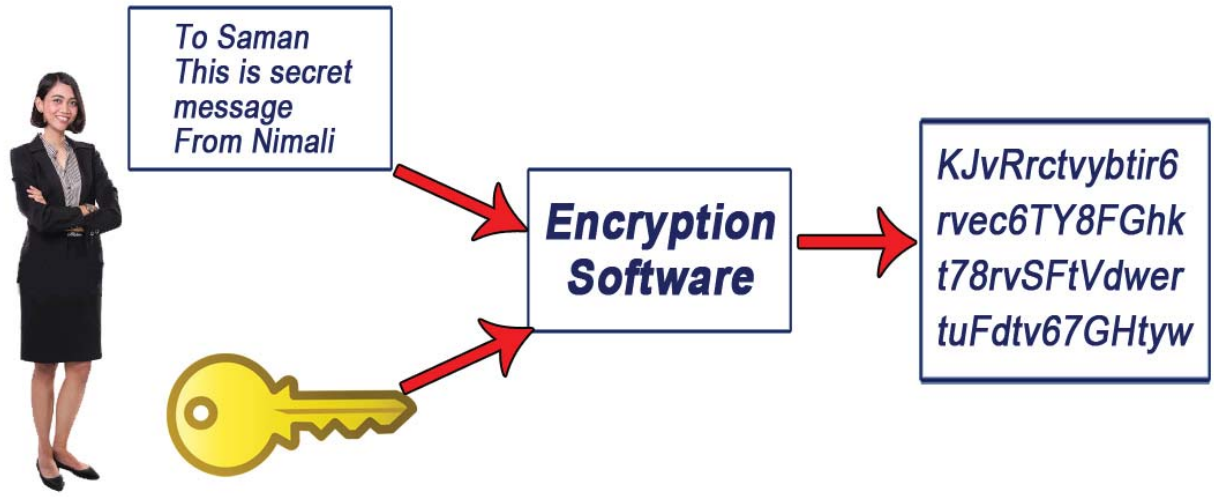
නිදසුනක් ලෙස, නිමාලිට සමන් වෙත වැදගත් පණිවුඩ යැවීමට අවශ්‍යය නම්, ඔහු පහත සඳහන් පියවරයන් අනුගමනය කළ යුතුවේ.

පළමුව නිමාලිට රහස් යතුරක් (key) ජනනය කිරීමට අවශ්‍යය වේ. එම යතුර සාමාන්‍යයයෙන් ඉතා දිගු random වූ අංකයකි.

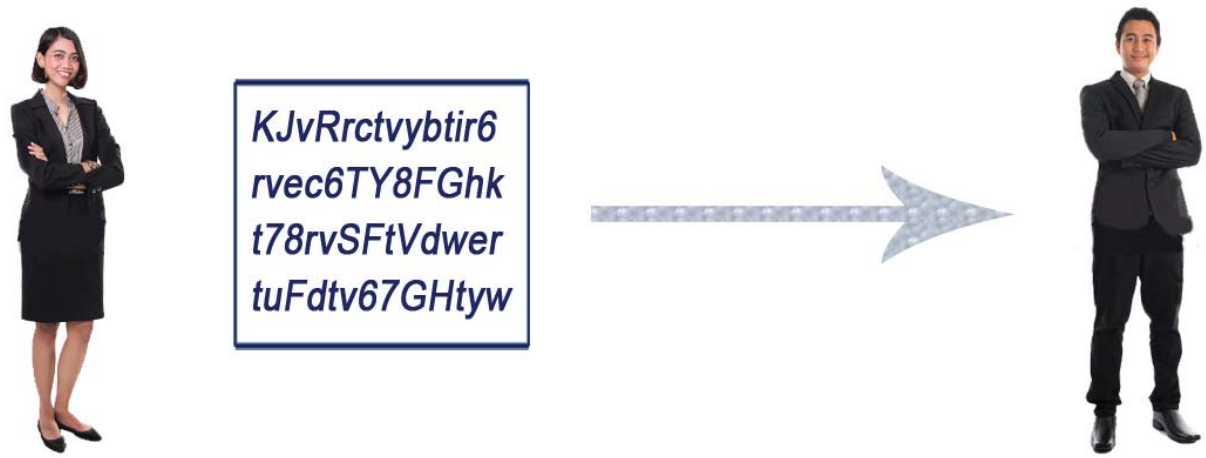
නිමාලි විසින් මෙම යතුරෙහි පිටපතක් සමන් වෙත ලබා දිය යුතුය. එසේම නිමාලි වෙන කිසිවකුට යතුර ලබා නොදෙන බවට වග බලා ගත යුතුවේ. (ඒ නිසා සමහරවිට නිමාලි සමන් වෙතට ගොස් USB Flash ක් භාවිතයෙන් එම යතුර ලබා දෙනු ඇත) දැන් සමන්ට යතුරේ පිටපතක් (copy of this key) නිමාලි ලබා දී මෙන් පසු ඇයට ආරක්ෂාකාරීව පණිවුඩය යැවිය හැකි-වේ. එනම් ඇයට විශේෂ encryption software සහ secret නැහ භාවිතා කර පණිවුඩය encrypting කළ පසු සමන් වෙත යැවිය හැකිවේ.



random letters සහ numbers වලින් encrypted පණිවුඩය (message) සමන්විත වේ. ඉන්පසු නිමාලි විසින් encrypted පණිවිඩය (message) සමන් වෙත පහත පරිදි යවනු ලැබේ.

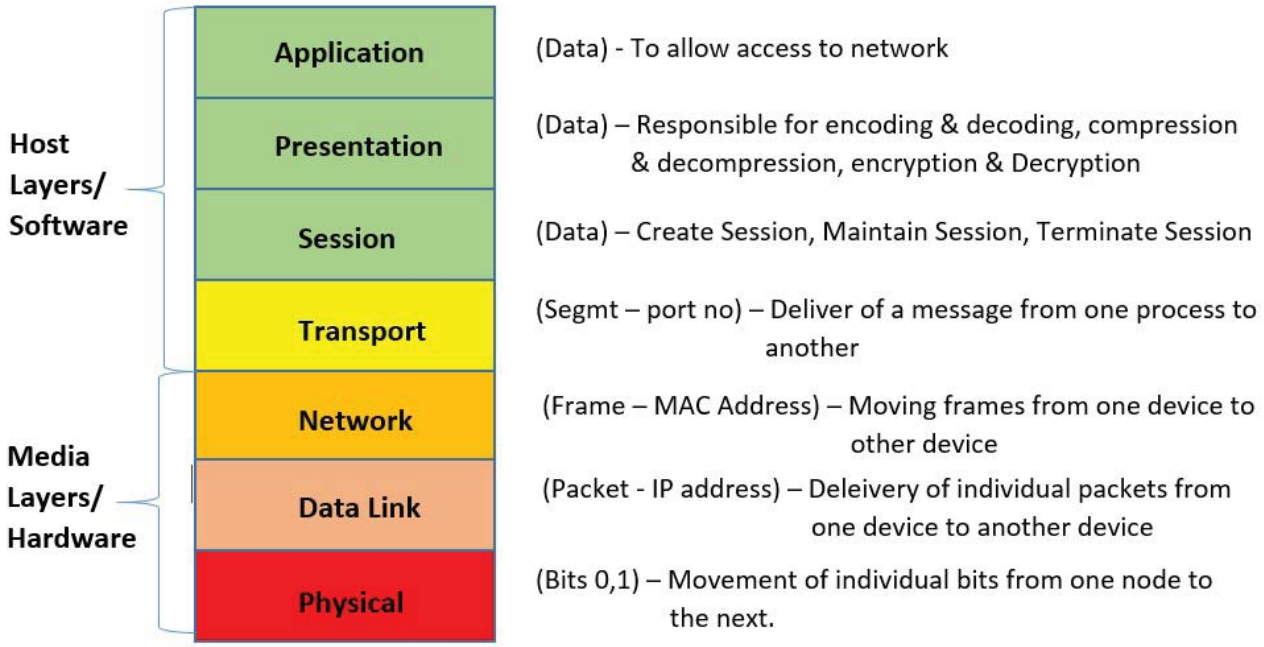


මෙම පණිවිඩය සමන් වෙත යැවීමට අන්තර්ජාලය වැනි පොදු (public) ජාලයක් භාවිතා කරනු ලැබුවද, එම පණිවිඩ Hacker මගින් සොරකම් කළද, ඒවා සංකේතාත්මක (encrypted) පණිවිඩයක් බැවින් එයට අදාල key නොමැතිව කියවීම හෝ තේරුම් ගැනීමට නොහැකි බව මෙහි විශේෂයයි.

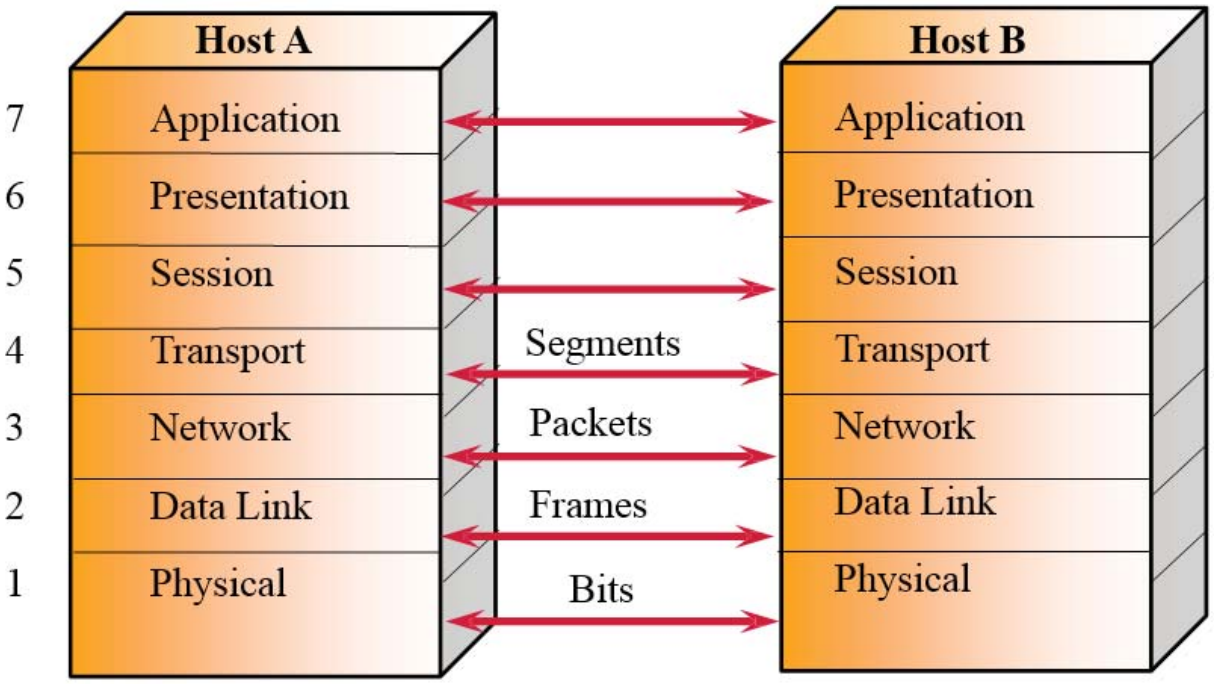


සමන්ට පණිවිඩය ලැබුණු විට ඔහු පණිවිඩය කියවීමට හැකි ලෙස (encrypt) කිරීමට විශේෂ රහස් කේතන මෘදුකාංගයක් (special decryption software) සහ රහස් යතුරක් (secret key) භාවිතා කරනු ලබයි.

OSI model අද්‍යාල පහත පෙන්වා දී ඇති පරිදි එහි ලේයර් හත පිළිබඳව අපි තව දුරටත් අධ්‍යයනය කරමු.



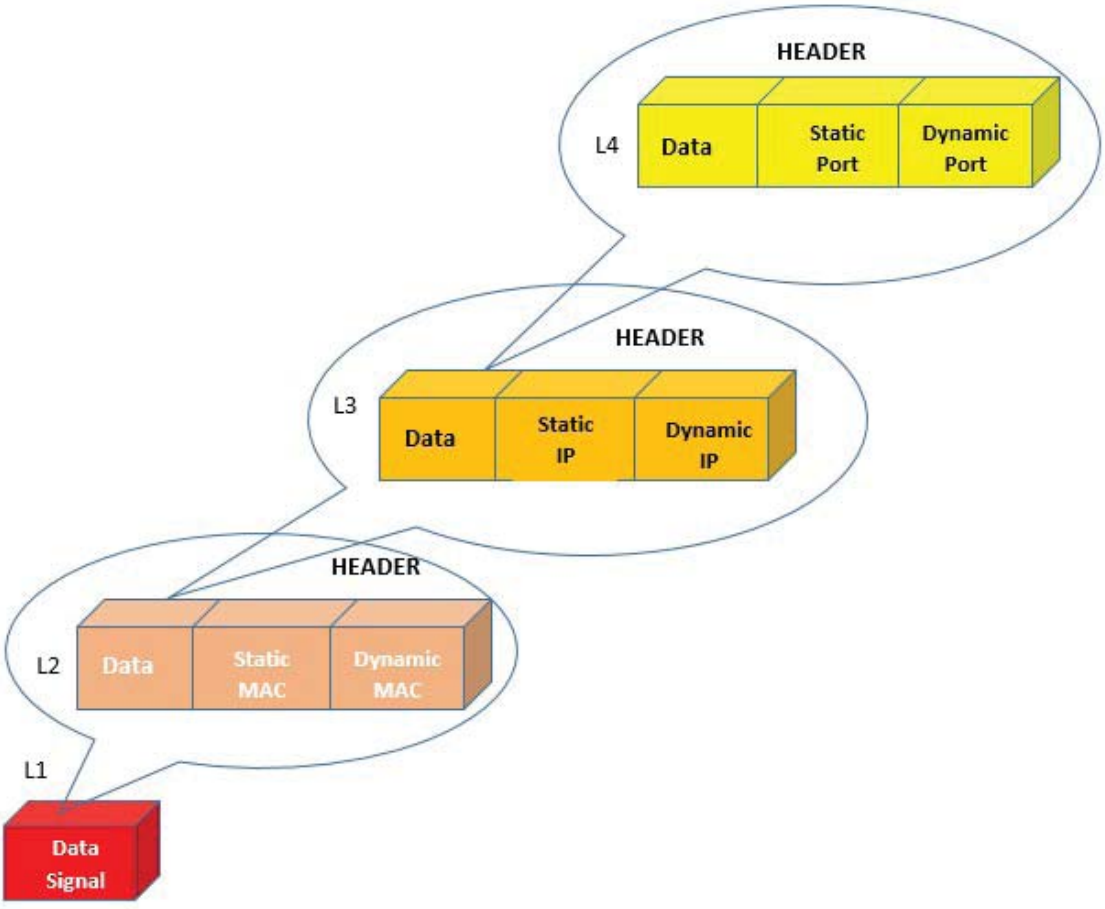
දත්ත Segments, Packets, Frames සහ Bits තොරතුරු OSI Layers මත පවතින අයුරු පහත රූපසටහනින් පෙන්නුම් කරයි.



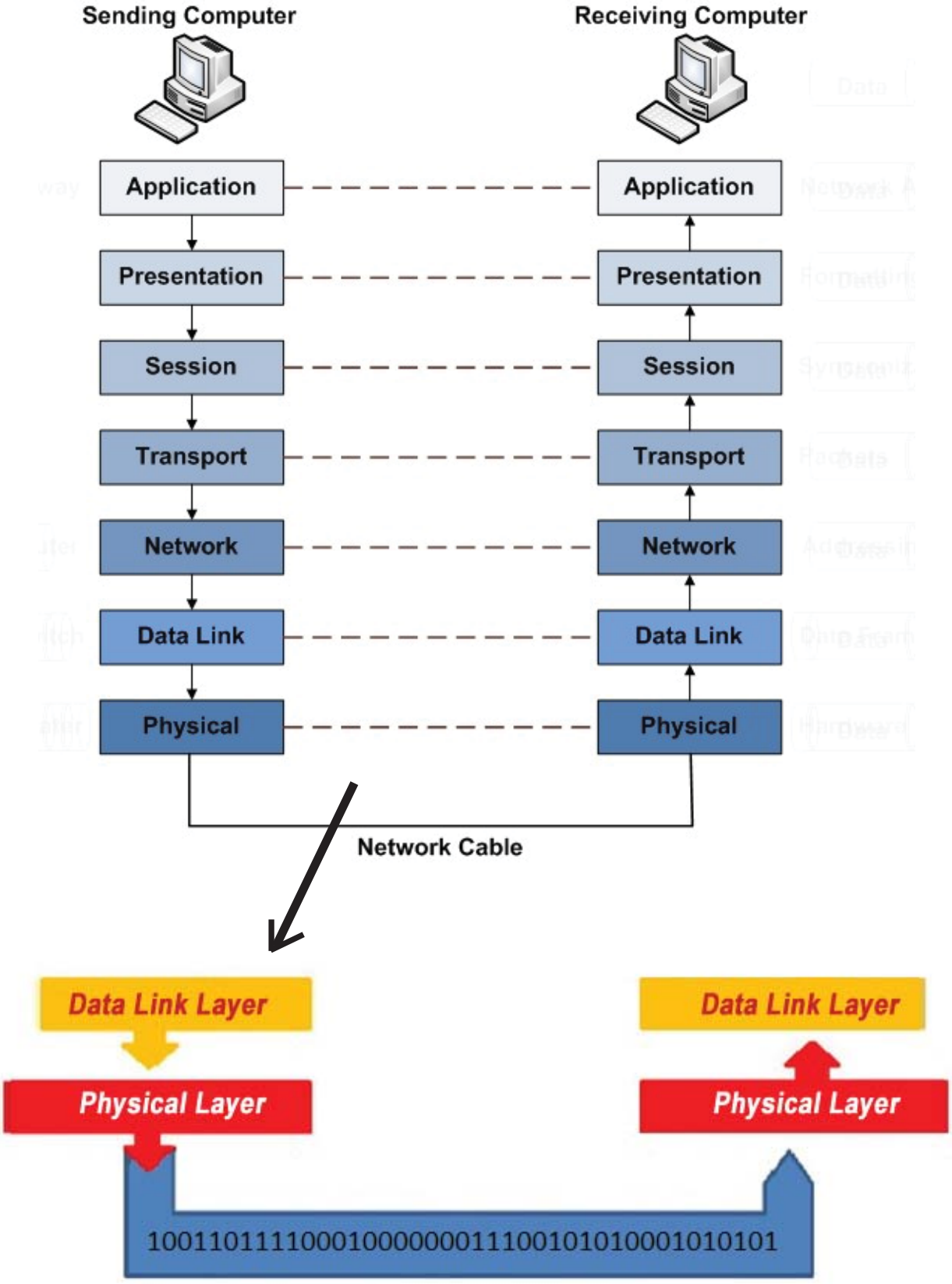
OSI model එකක් ගත් විට data packet එකක් මොන මට්ටමේ ඇති layer එකක සිට යැව්වත් එය ගමන් කරන්නේ යට ඇති stages වලටය. අවසානයේදී physical layer එක හරහා communication media එකට එනම් දත්ත ගෙන යන මාධ්‍යට ලඟා වෙනු ලබයි. මෙසේ Communication media එක හරහා ගමන් කල යුතු දුර ගමන් කර අවසන් වූ කල්හි නැවතත් පෙර පරිදිම physical layer එකේ සිට උඩට ඇති stage වලට ලඟා වී අවසනදී data packet එවන ලද layer එකට සමාන layer එකට ගොස් දත්තය අනෙක් පරිගණකයෙන් පෙන්වනු ලබනවා.

මෙය ඉතා ක්ෂණිකව සිදුවන ක්‍රියාවලියක් වන අතර තනි layer දෙකක් අතර දත්ත හුවමාරුවනවා වැනි අදහසක් ලබා දෙයී නමුත් මෙම process වන ක්‍රියාවලිය layer ගණනාවකින් යුක්තව සංකීර්ණ ක්‍රියාවලියක් සිදුවනු ලබයි.

OSI Layers මත පවතින දත්ත Segments (L4), Packets (L3), Frames (L2) සහ Bits (L1) අභ්‍යන්තරයේ ක්‍රියාකාරීත්වය පහත අයුරින් පෙන්විය හැකිය.



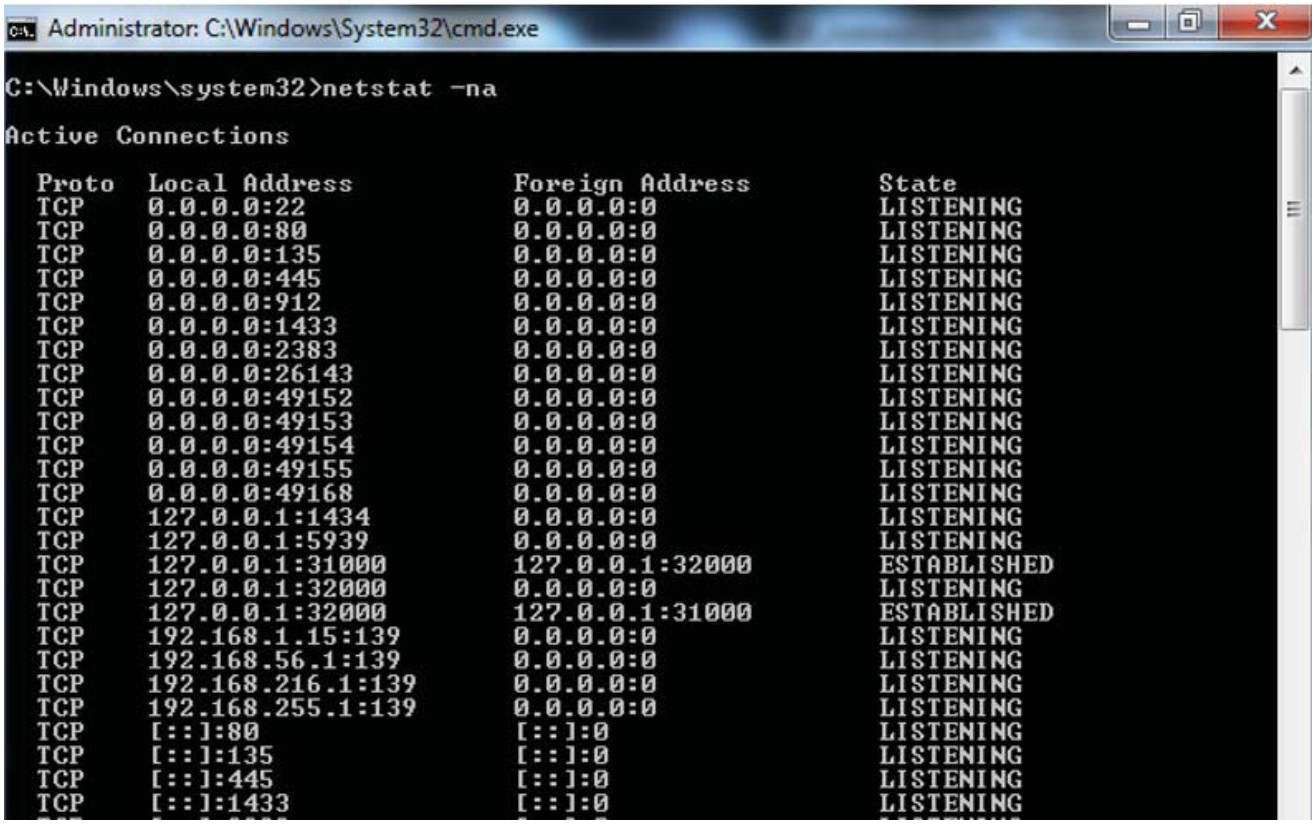
පරිගණක දෙකක් අතර OSI Layer යේ ක්‍රියාවලිය පහත පරිදි පෙන්වා දිය හැකි වේ.



Port Addresses හඳුනා ගනිමු

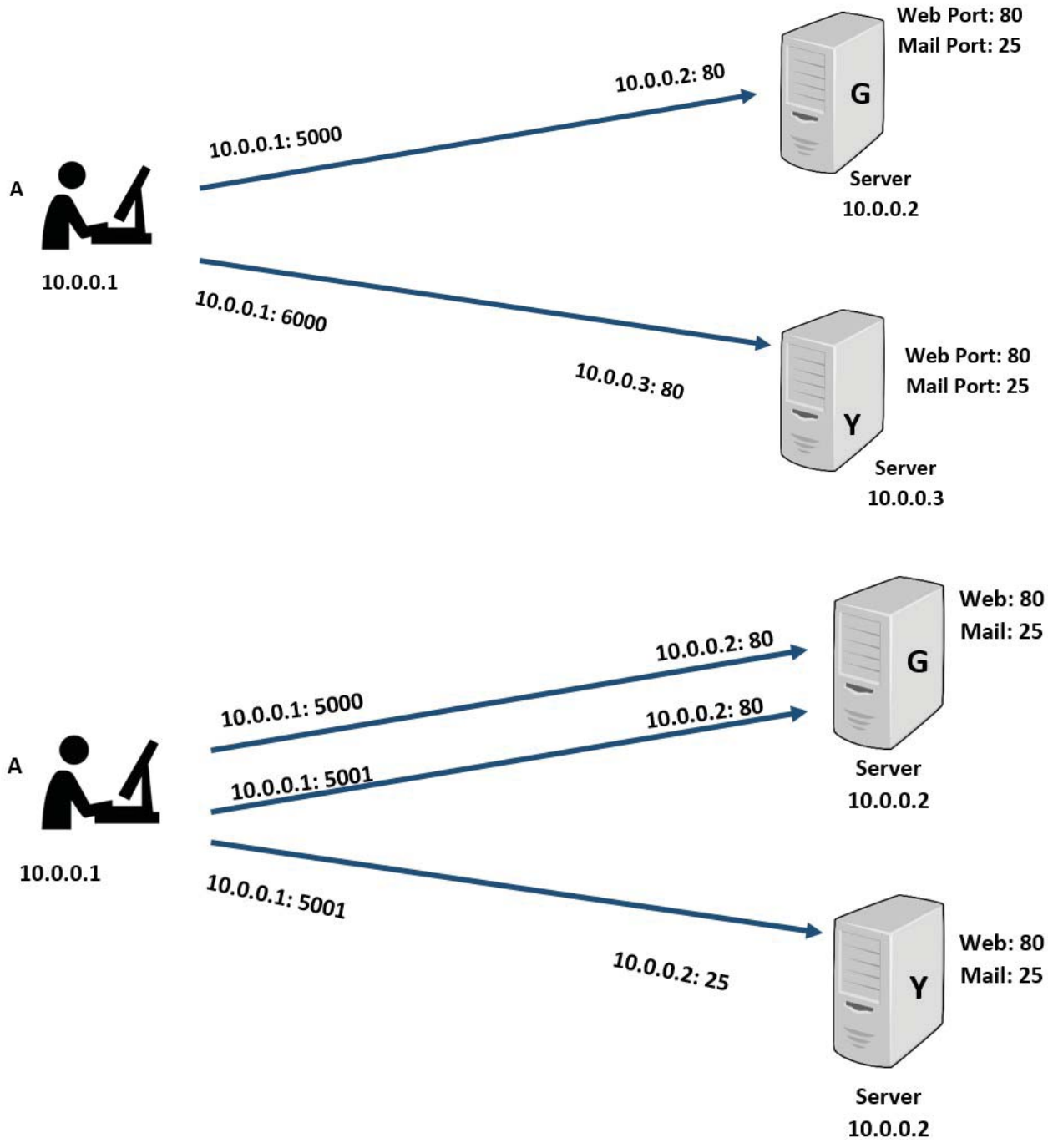
මෙම Address වර්ගය 16 bits විශාලත්වයක් (එනම් 2 bytes) ගනු ලබන අතර එය පූර්ණ සංඛ්‍යා පරාසය 0 සිට 65535 දක්වා විහිද පවතී.

පරිගණකයට අදාල තොරතුරු එක් device සිට තවත් device ගමන් කිරීමේ ක්‍රියාවලිය හඳුනා ගැනීමට (identify the process) මෙම මෙම Address භාවිතා කරයි. OSI ආකෘතියේ Transport Layer ස්තරය මෙහිදී භාවිතා වේ.



තව දුරටත් Port Address පිළිබඳව විග්‍රහකර බැලීමේදී Port No 1 සිට 1023 දක්වා ඇති සියල්ල අප නිතර පරිගණක ක්ෂේත්‍රයේ භාවිතා කරන අතර (Well know port Nos) Port No. 1025 - 65535 දක්වා ඇති සියල්ලම ports Private Port නැති නම් Dynamic නමින් හඳුන්වයි.

Port Address පහත පරිදි IP Address සමග එකතු කිරීම Socket ලෙස නැත්නම් Combination of IP Address + Port No ලෙස උදාහරණයක් වශයෙන් පහත පරිදි 10.0.0.1: 5000 පෙන්වා දිය හැකිය.



Logical Addresses

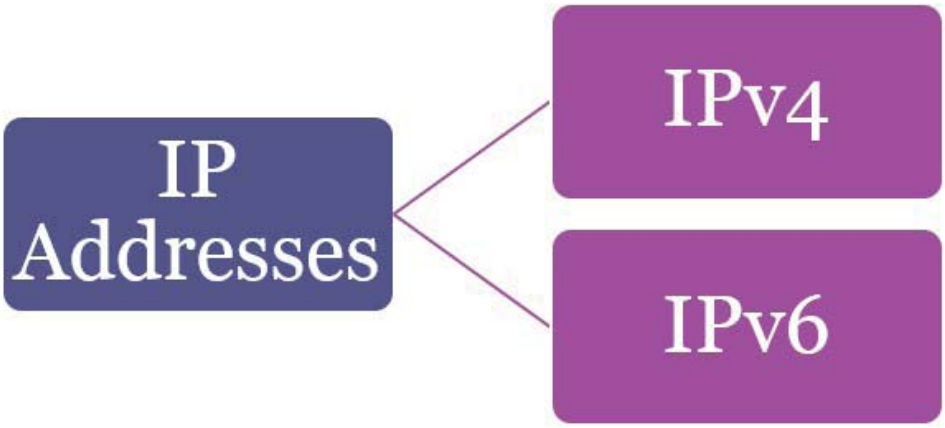
තාර්කික ලිපින වැඩි වශයෙන් ඡේද ලිපිනයක් (addresses) ලෙස හැඳින්වේ. OSI මොඩියුලයේ Network Layer තුළ Logical Addresses ලෙස මෙම Address වර්ගය භාවිතා වේ.

ඕනෑම පරිගණකයක් හෝ අන්තර්ජාලයට සම්බන්ධ වූ router උපාංගයට වුවද එයටම වෙන්වූ IP ලිපිනයක් තිබිය යුතුය.
IP ලිපිනය යනු ඕනෑම host අන්තර්ජාලය හා සම්බන්ධ වීමේදී වෙන වෙනම හඳුනා ගැනීමට භාවිතා කරයි.

IPv4 (IP version 4) හඳුනාගනිමු

IP addresses ප්‍රධාන සංස්කරණයන් දෙකකින් පවතී.

- IP version 4 (IPv4) address 32 bits ප්‍රමාණයක් දිගු වේ එනම් 4 bytes වේ.
- IP version 6 (IPv4) address 128 bits ප්‍රමාණයක් දිගු වේ එනම් 16 bytes වේ.



IPv4 Address වර්ගය අන්තර්ජාලය තුල ඇති IP Address අතුරින් වඩාත් පුළුල් ලෙස භාවිතා වේ. එසේම IPv6 භාවිතය අන්තර්ජාලය තුල සෙමින් වර්ධනය වේ.
වර්තමානයේ අප IPv4 සිට IPv6 දක්වා සංක්‍රමන අවධියෙහි සිටින බැවින් IPv4 පිළිබඳ පුළුල් අවබෝධයක් සහ IPv6 හඳුන්වාදීමට හේතු වූ සීමා-වන් දැන ගැනීම වැදගත් වේ.

ජාලකරණයේ භාවිතාවට ගනු ලබන Network DOS Commands

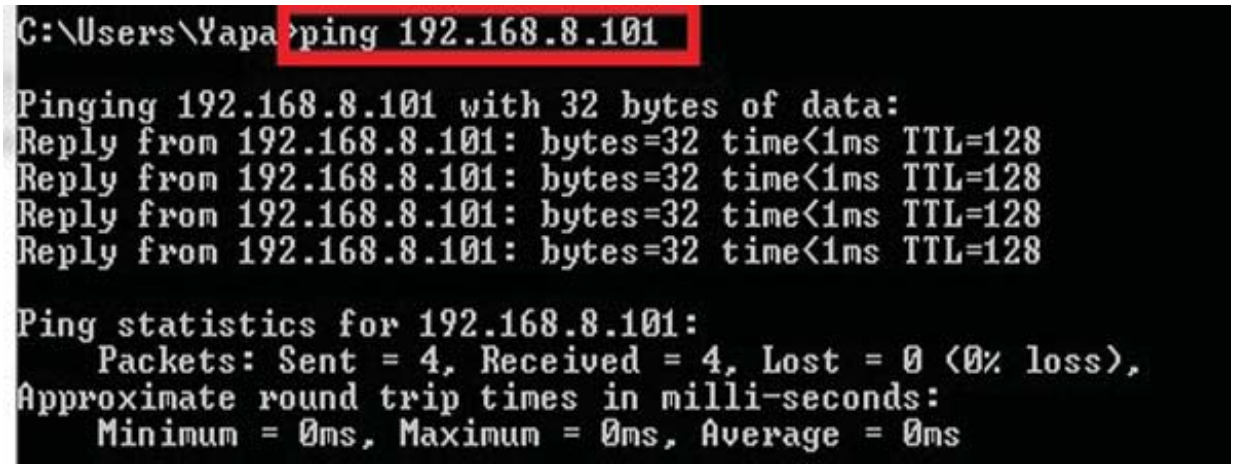
1. Ping Command භාවිතා කරමු

මෙම ping command මගින් IP-level මට්ටමෙන් ජාලය අතර ඇති connectivity තත්ත්වය verify කර ගැනීම සිදුවේ. විශේෂයෙන් ඔබ වැඩ කරමින් සිටින ජාලයට සවි වන cable හෝ LAN socket එකට සම්බන්ධවන ස්ථානයේ නිසි ලෙස පරිගණකයට හෝ වෙන යම් ජාල උපාංගයකට සම්බන්ධ නොවී ඇති දැයි පහත අයුරින් සොය බැලිය හැකි වේ.

මෙහිදී සිදුවනුයේ ICMP echo request එකක් target host name හෝ IP address යවනු ලැබීමය.

මීට අමතරව පහත විධානය භාවිතා කර txt file එකකට එම තොරතුරු සියල්ල ලබා ගත හැකිවේ copy command to txt file.

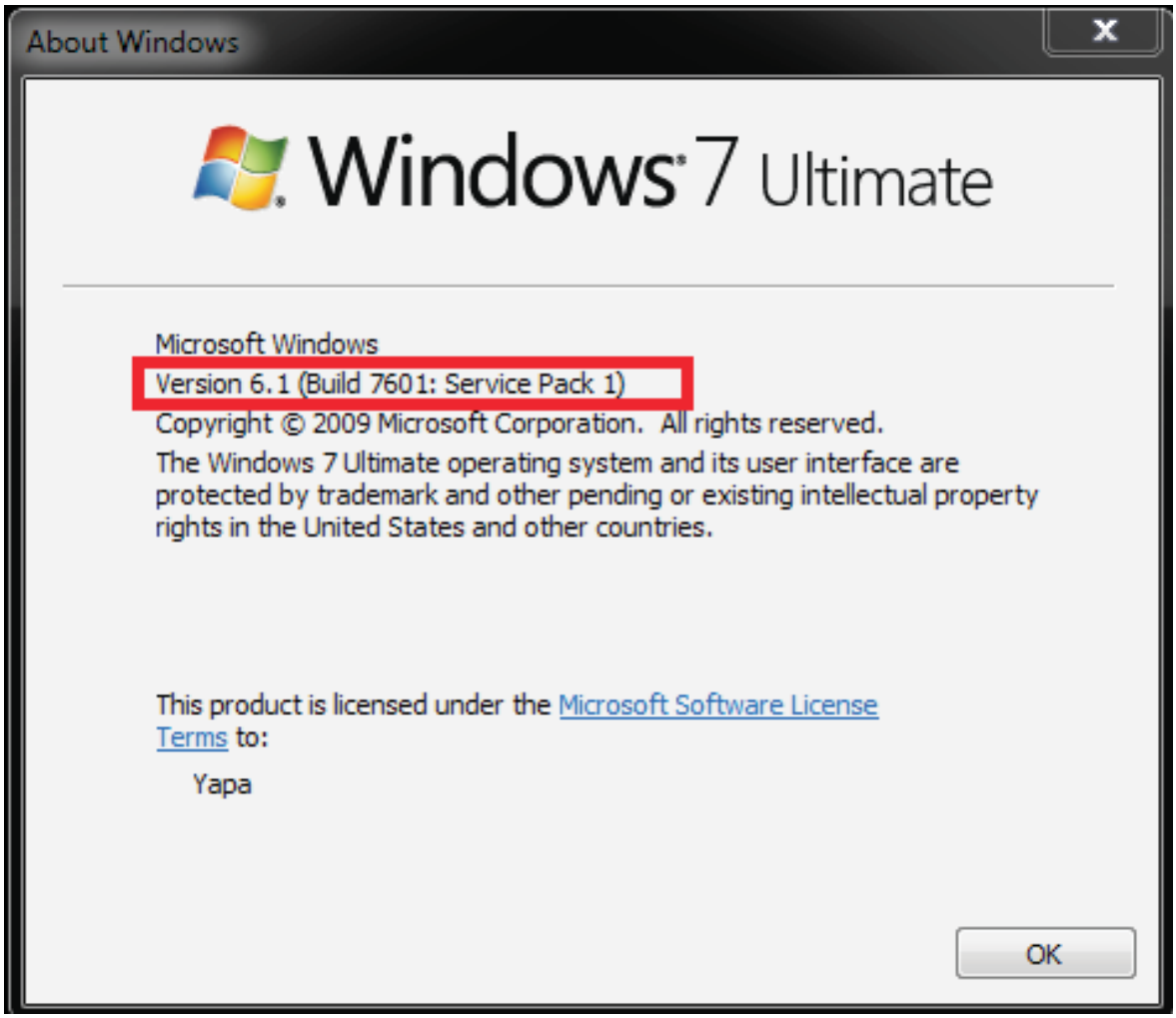
ping 192.168.100.1 -t >> c:\ping.txt



2.

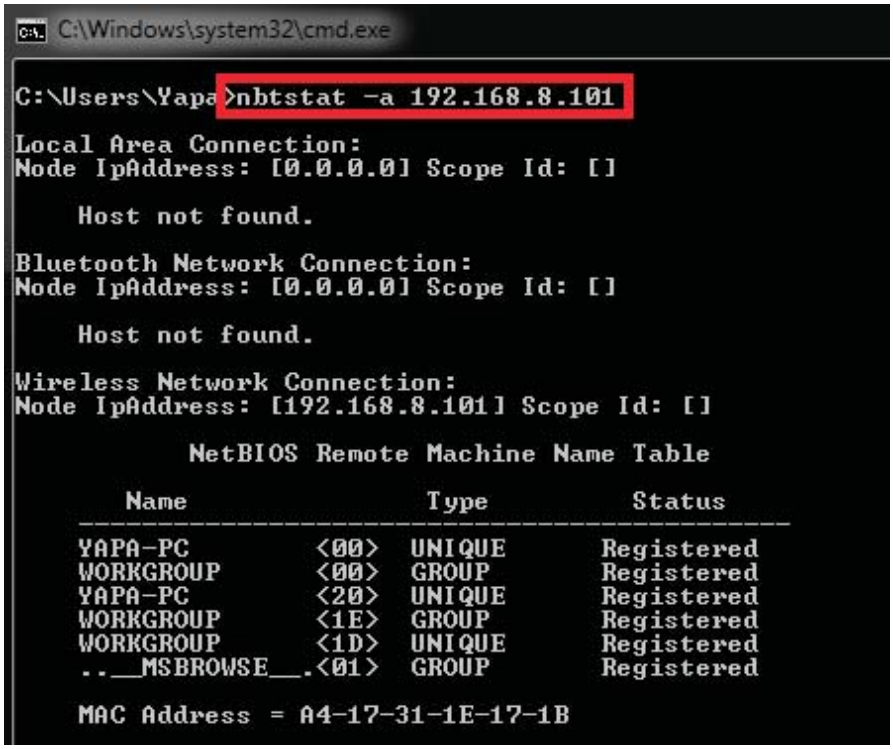
පරිගණකයේ Memory Size සොයා ගැනීමට අවශ්‍ය නම් පහත පරිදි wmic විධානය ලබා දිය යුතුවේ. මෙම command එක Windows කළමනාකරණ උපකරණ පිළිබඳ විධාන රේඛාව ලෙස හඳුන්වයි. WMIC - Windows Management Instrumentation Command-line.

3. පරිගණකයේ Windows Edition සහ Build Number ඔබට සොයා ගැනීමට අවශ්‍ය නම් පහත අයුරින් "winver" විධානය, පරිගණකයේ Run box තුලට (Key + R) හෝ DOS Command ලෙස type කල යුතුවේ.



4. පරිගණකය ක්‍රියාකරන ජාලය තුල ඇති තවත් පරිගණකයක නාමය සොයා ගැනීමට අවශය වූ විටකදී පහත අයුරින් ඔබ එහි IP Address දන්නේ නම් nbtstat -a <IP address> එක type කරන්න. එවිට එම පරිගණකයේ නම සොයා ගත හැකිවේ (Finding computer name using IP). මෙහිදී NetBIOS පිළිබඳ තොරතුරු TCP (NBT) සම්බන්ධතා හරහා ප්‍රදර්ශනය කරයි.

nbtstat -a 192.168.8.101



5. පරිගණකයට සවිකර ඇති සියලුම adapters වල සම්පූර්ණ සාරංශයක් මෙම විධානය භාවිතා කර ලබා ගත හැකිවේ.
එනම් ipconfig/ all විධානය යෙදීම මගින් TCP/IP network configuration values, DHCP සහ DNS වල settings ද මීටත් අමතරව IP address, subnet mask සහ default gateway වල අගයන්ද ලබා ගත හැකිවේ.

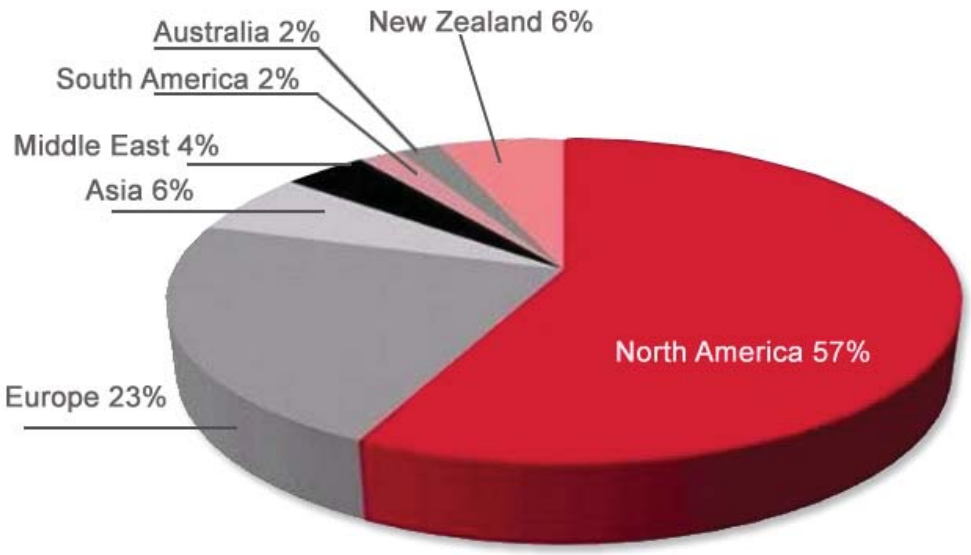
2

හැකර් (hacker) යනු කුමක්ද ?

Hacking ලෙස හඳුන්වන්නේ අනවසරයෙන් පිවිසීමක් හා අන්සතු දෙයක් හොරකම් කිරීමකි. තවත් අකාරයකට පවසනවා නම් වෙනත් පරිගණකයකට හෝ පද්ධතියකට හෝ ජාලයකට අනවසරයෙන් ඇතුලත් වීම හැකින් (Hacking) ලෙස හදුන්වයි.

පරිගණක ජාලකරණය හා සහ සම්බන්ධ පද්ධති සාමාන්‍ය හැසිරීම මෙහෙයවනු ලබන්නේ කිසියම් තාක්ෂණික උපාය මාර්ගයකිනි. හැකර් වරයා නිරන්තරයෙන්ම ඕනෑම පුද්ගලයෙකු වේ. මෙම පදය චෛතිහාසිකව වශයෙන්ම පරිගණක පද්ධති හා සම්බන්ධ නොවූ අතර නිර්මාණාත්මක, දක්ෂ තාක්ෂණික වැඩ සටහන් ලොවට බිහිවීමත් සමග මෙම “හැකින්” චිළිදැක්වුමකි. එනම් මීට වසර 50 කට අදික කාලයකදී මෙම ක්‍රියාවලිය ආරම්භ වන ලදී කෙසේ වෙතත්, අද බාල සහ තරුණ මෙන්ම මහලූ පුද්ගලයින් අනවසරයෙන් වඩාත් සුලබව අන්තර්ජාලයේ අනිෂ්ට වැඩසටහන් පවත්වාගෙන යන අතර තම තමන්ට වෙන්වූ හැකින් ක්‍රමවේදයෙන් හා වෙන් වෙන්වූ ජාල සමග සම්බන්ධව හැකර්වරුන් ලොවට ප්‍රවිෂ්ට වී ඇත.

ලෝකය තුල Hacking ව්‍යාප්ත වී ඇති අයුරු පහත ප්‍රස්තාරයෙන් නිරූපණය කරනු ලැබේ.



ප්‍රධාන හැකර්වරුන් හඳුනා ගනිමු (Main Types of Hackers)

මෙම හැකර්වරුන් ප්‍රධාන කොටස් 3 කට වෙන් කරන්න පුළුවන් වේ.

1. White Hat Hacker / සුදු තොප්පි හැකර්වරු
2. Black Hat Hacker / කලු තොප්පි හැකර්වරු
3. Grey Hat Hacker / අළු තොප්පි හැකර්වරු

White Hat Hacker හෙවත් සුදු තොප්පි හැකර්වරු (Good Guys)

පරිගණක සහ ජාල ආරක්ෂක ප්‍රමුඛයන් ලෙස හැඳින්වෙනු ලබයි. මොවුන් සිය දැනුම සිය ආයතනයේ පරිගණකවල හා ජාලවල ආරක්ෂාව උදෙසා වැඩ කටයුතු සිදු කරයි. මොවුන් පද්ධතියකට අනවසරයෙන් ඇතුළු වූවත් ඒ අවශ්‍ය ම හේතුවක් නිසා පමණක් වන අතර සෑම විටම හානිකර හැකර්වරුන් ගෙන් පරිගණක පද්ධති බේරා ගැනීම මුඛ්‍ය පරමාර්ථය කොට වැඩ කරයි. මෙවුන් Computer Security experts ලෙස හඳුන්වනු ලැබේ.

Black Hat Hacker හෙවත් කලු තොප්පි හැකර්වරු (Bad Guys)

මොවුන් සැගවී ජීවත් වනු ලබන අතර පරිගණක වලට සහ ජාල වලට නීති විරෝධී හා අනවසර ඇතුළු වීම් සහ ඒවාට හානිකර කටයුතු සඳහා භාවිතයට ගනු ලබයි. පරිගණක ජාල අවුල් කරන්න, මුදල් උපයන්න සහ අනවසර දත්ත ලබා ගන්න වගේ මේ දේවල් වලට තමයි මෙම Black Hat Hacker උත්සාහ දරනු ලබනු යේ. බැංකු වල ගිණුම් තොරතුරු “credit card” තොරතුරු සොරකම් කිරීම සහ වෙබ් අඩවි වල ප්‍රතිරූපය විනාශ කිරීම මෙය හා සම්බන්ධ උදාහරණ කිහිපයකි.

Brute-force Attack

ප්‍රහාරකයකු විසින් බොහෝ මුරපද (passwords) හෝ මුරවචන (passphrases) උපකල්පනය කරමින් ඒවා නිවැරදිව භාවිතා කිරීම brute-force attack ලෙස හඳුන්වා දෙනු ලැබේ. ප්‍රහාරකයා විසින් නිවැරදි එක සොයාගන්නා තුරු සියලුම මුරපද සහ මුරවචන යම් ක්‍රමවේදයකට පරීක්ෂා කර බලනු ලැබේ.

මෙම වර්ගයේ ප්‍රහාරයන් සිදුකරනු ලබන්නේ ජාලය තුලට ඉදිරි පසින් (Front door) හරහා පැමිණීමෙන්ය. මෙය trial-and-error ලෙසට system's password උපකල්පනය (guess) කිරීම සිදු කරනු ලැබේ. ජාල ප්‍රහාරයන්ගෙන් හතරෙන් එකක් Brute-force attack වේ. ස්වයංක්‍රීය මෘදුකාංග බොහෝ විට සිය දහස් ගණනක මුරපද එකතුව අනුමාන කිරීමට උපයෝගී කර ගනී.

මෙම ප්‍රහාරය වලින් වැලකී සිටීමට නම් ඔබගේ ගිණුමට login වීමට භාවිතා කරන login attempts ප්‍රමාණය සීමා කිරීමය නැතිනම් ගිණුම lock වීමට ඉඩ හැරීමයි. ගිණුමට login වීමට උත්සාහයන් කීපයක්ම අසාර්ථක වූ පසු එයට භාවිතා කරන ලද IP Addresses භාවිතය Block කිරීම ද සිදු කල හැකිවේ.

Ethical Hacker කෙනෙකු වීමට අවශ්‍යය නම් පහත දක්ෂතාවයන් ඔබට තිබිය යුතුවේ.

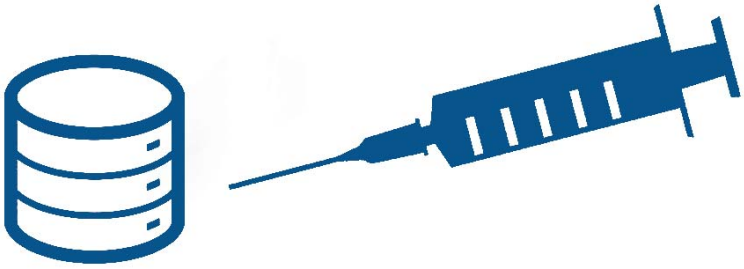
- නිර්මාණශීලීත්වය (Creativity).
- ඉගෙන ගැනීමට තිබෙන අවශ්‍යයතාවය (Will to learn).
- මනා ලෙස දැනුමෙන් බලසම්පන්න වීම (Knowledge is power).
- ඉවසිලිවන්තකම (Patience).
- විශිෂ්ඨ හැකර්වරයෙක් ලෙස (elite hacker) සලසුම් (Programming) කිරීමට හැකිවීම .

SQL Injection Attack

මෙම වර්ගයේ attacks buffer overflows in system code නොහොත් injection attacks ලෙසින් මීට බොහෝ කාලයකට පෙර සිට වෙබ් ලෝකයේ භාවිතයට ගනු ලැබේ. මීට අමතරව වෙනත් වර්ග වල code injection attacks දක්නට ලැබේ. SQL injection වර්ගය ද මෙයින් එක් වර්ගයකි.

මෙහිදී අප දැන ගත යතු වන්නේ basic commands need to run an SQL injection සහ how it can be used to bypass basic web application authentication.

මෙම injection attacks විවිධ වර්ගයේ ක්‍රියා වන් සඳහා භාවිතා වේ. Bypassing authentication, manipulating data, viewing sensitive data and even executing commands on the remote host.



Hacker කෙනෙකු වීමට මිනිසුන් යොමු වීමට හේතු,

විනෝදයට (Just for fun).
පේත්තුකරුවක් ලෙස හැසිරීම සඳහා (Show Off).
වෙනත් පද්ධති රහසිගතව හැක් කිරීම සඳහා.
බොහෝ අයට අවශ්‍යයවන ඔවුන්ගේ අදහස් ප්‍රකාශ කර ගැනීමට.
වැදගත් තොරතුරු සොරකම් කර ගැනීමට.
යුද්ධයක් වැනි අවස්ථාවලදී සතුරාගේ පරිගණක ජාල විනාශ කර දැමීමට

ක්‍රැකර්වරු (Cracker) හඳුනා ගනිමු

ජාලය මත ක්‍රියා කරන තව කෙනෙකුගේ පරිගණක පද්ධතියක් බිඳ දමන පුද්ගලයෙකු cracker ලෙස හඳුන්වා දෙනු ලබයි. පරිගණක වැඩසටහන් වලට අදාළ passwords හෝ licenses මග හැර යාම (bypass) හෝ වෙනත් ආකාරයකින් හිතා තාම පරිගණක ආරක්ෂණ කඩ කිරීම් වැනි දෑ මෙය මගින් ප්‍රකාශ වනු ලබයි. One who break into systems illegally are crackers.

හැක් වීමක් සිදු වූ පසු කළ යුතු දේ ?

- ඔබගේ පරිගණක ජාලය තුල Hacked වීමක් සිදු වී ඇත්නම් පහත පෙන්වා දී ඇති පරිදි එයින් ඉදිරියට සිදු විය හැකි විනාශය වළක්වා ගැනීමට උත්සාහ කරන්න.

- පද්ධතියට සම්බන්ධ වන සියලු ම උපාංග වසා දමන්න. (Shutdown the system)

- ඔබගේ පද්ධතිය ජාලය හා තිබෙන සම්බන්ධයෙන් වෙන් කරන්න. (Separate the system from network)

- සියලු වැඩසටහන් නැවත යථා තත්ත්වයට පත් කිරීම හෝ backup භාවිතා කර පද්ධතිය නැවත ප්‍රතිසංස්ථාන (Restore) කරගන්න.

- සිදුවූ සියල්ල පිළිබඳව ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදයේ හෝ ශ්‍රී ලංකා පොලිසිය අමතා ඔවුන්ව ඒ පිළිබඳව දැනුවත් කරන්න.

3

මෙම විනිවිදුම් පරීක්ෂාව (Penetration Testing)

මෙය පරිගණක ජාල ආරක්ෂණය ඇගයීමට ලක් කරන ක්‍රමවේදයකි. මෙම පරීක්ෂාව සත්‍යය ලෙසම පරිගණක පද්ධතියකට හෝ ජාල පද්ධතියකට බාහිර ව සහ අභ්‍යන්තර ව සිදුවන ප්‍රහාරයන් simulate කර එම තර්ජන පිළිබඳ සොයා බැලීමේ ක්‍රමවේදයයි.

සජීවී විශ්ලේෂණ ක්‍රියාවලියක් සම්බන්ධ කර ගැනීමේ දී ඕනෑම විභවය-ක් අනතුරට භාජනය විය හැකි අතර එහි ප්‍රතිඵලය ලෙස දුර්වල හෝ අවිධිමත් පද්ධති පිහිටා ඇති ආකාර නිසා ද ඒවා පිළිබඳ දැනුවත්ව සහ නො දැනුවත් ව කම යන දෙකම නිසා හෝ දෘඩකාංග/ මෘදුකාංග වල ඇති අඩුපාඩු නිසා හෝ එම ක්‍රියාවලින් තුල තාක්ෂණික වශයෙන් අවදා-නම් ක්‍රියාකාරීත්වයක් ඇතිවිය හැකි ආකාරයේ දුර්වලතාවයන් වලින් යුතු මෙහෙයුම් පද්ධතිය වැනි දෑ සඳහා මෙවැනි attacks වලට ගොදුරු විය හැකි වේ.

පහත විශ්ලේෂණය මගින් යම් විභවයක් ඇති attacker කෙනෙකු හට ඉදිරියේ දී ඔහුගේ එම ප්‍රහාරය දියත් කරගැනීම සඳහා උදව් ලබා දෙනු ලැබේ. එහිදී ජාලයේ සහ උපකරණ වල ආරක්ෂාකාරීත්වය, අනතුරකට භාජනය විය හැකි ක්‍රමවේදයන් (vulnerabilities) සහ සජීවී උපයෝජනය (exploitation) යන ක්‍රියාවලින් පිළිබඳව පැහැදිලි කර දෙනු ලබයි.

Penetration පරීක්ෂණ හරහා ආරක්ෂකාරීත්වයට ඇති වන ගැටළු සොයා බලා ඒවා පරිගණක පද්ධතියේ හිමිකරු වෙත දැනුම් දීම මෙහිදී සිදු කරනු ලබයි. ආයතනයේ දියුණුවට සහ එහි ඵලදායිතාවට බලපාන අයුරින් එම ස්ථානයට වැදගත් වන penetration test පරීක්ෂාව සිදුකරන අතර මෙම තොරතුරු එකට එක් කර එය නිවැරදි තක්සේරුවක් ලෙස ඉදිරිපත් කරමින් ඔබේ ආයතනය Hack වීමෙන් ඇති විය හැකි භයානක උප ද්‍රව්‍ය වලින් සිදුවීමට යා හැකි විනාශයන් අවම කර ගත හැකිය.

Penetration පරීක්ෂාවේ ක්‍රමවේදයන්

මෙහි දී මෙම පරීක්ෂාව ක්‍රමවේදයන් දෙකකින් සිදු කරනු ලබයී.

1) Internal පරීක්ෂාව

භෞතිකමය සහ තාර්කික අංශ දෙක ඔස්සේ ඇති වෙනස් ජාල වල ප්‍රවේශ ස්ථාන වලින් මෙම පරීක්ෂණය සිදු කරනු ලබයි. මෙය වඩාත් සවිස්තරාත්මක ලෙස ආරක්ෂාකාරීත්වය පිළිබඳ තොරතුරු ලබා දෙනු ලබන පරීක්ෂාවකී

2) External පරීක්ෂාව

මෙම පරීක්ෂණයේ මූලික අරමුණ වනුයේ යටිතල ව්‍යුහය (infrastructure), පරිගණක Servers සහ මෘදුකාංග කෙරෙහි අවධානය යොමු කිරීම් ය.

මීට අමතරව අන්තර්ජාලය උපයෝගී කර ගනිමින් මෙහි තොරතුරු පිළිබඳ විස්තරාත්මක විග්‍රහයක් ලබා දෙනු ලැබේ. ජාල ගණනය කිරීම් සහ එහි විශ්ලේෂණ ද මෙයට ඇතුලත්වේ. Filtering devices වන firewalls සහ routers වැනි උපාංග වල vulnerabilities සොයා ගැනීම සඳහා ඉතා සියුම් ලෙස පරීක්ෂණ සිදු කරනු ලබන අතර එහි ප්‍රතිඵල ලෙස ඔබ ආයතනය තුලට නිත්‍යානුකූල නොවන අයුරින් ප්‍රවේශ වීමෙන් සිදුකරනු ලබන විවිධ බලපෑම් නිසා ආයතනය විවිධ ප්‍රතිවිපාක වලට ලක් විය හැකි වේ.

ඉහත පරිදි විනිවිද යාමේ (Penetration) ක්‍රමවේදයන් දෙකක් ඇති නමුත් ඒවා තුල සිදු වන වෙනස්කම් සැලකිල්ලට ගනිමින් තුන් වර්ගයක පරීක්ෂණ ක්‍රම පහත අයුරින් පෙන්වා දිය හැකිවේ.

Penetration පරීක්ෂණ ක්‍රම (Test Type)

1) Black box ක්‍රමය

මෙම පරීක්ෂාව මගින් පරීක්ෂක තොරතුරු ලබාගත නොහැකි අතර ඒ නිසා මෙම පරීක්ෂාව වඩා හොඳ ක්‍රමවේදයක් ලෙස හැඳින්විය හැකිය. එසේම crackers and script kiddies අය පිළිබඳ තොරතුරු සෘජු වම ලබා ගැනීමේ හැකියාව නොමැතිකම ද එසේ ඉලක්ක ගත ආයතන වල තොරතුරු මහජන මූලාශ්‍ර වලින් එකතු කිරීම අශ්‍යතාවය ඔවුන්ට ඉටු නොවෙනු ඇත. මෙය සැබෑ ලෝකයේ දී ඇති විය හැකි ප්‍රහාරයන් (Attacks) අනුකරණය කරනු ලබයි.
Black Box පරීක්ෂාවට ජාල mapping, shares and services ගණනය කිරීම්, මෙහෙයුම් පද්ධති ඇගිලි සලකුණු අයත් වේ.

2) White box ක්‍රමය

ජාලයට සිසුවිය හැකි විශේෂිත ප්‍රහාර හෝ නිශ්චිත ඉලක්ක වලට විරුද්ධව ආරක්ෂාව තහවුරු කිරීමට අවශ්‍ය තොරතුරු සපයා දීම හෝ එය සිදු කිරීම මෙයට අදාළ වේ. මෙහිදී තෝරා ගත් ක්‍රමය වනුයේ එම සමාගම් වල ආරක්ෂාව පිළිබඳ සම්පූර්ණ විගණන සිදුකිරීමය.

3) Grey box ක්‍රමය

මෙම ක්‍රමවේදය මගින් testers හට යම් දැනුමක් ලබා දෙන අතර මෙම පරීක්ෂණ මගින් tester හට හොඳ ස්ථානයක් ලබා දීම ද සිදු කරනු ලැබේ. තවද මෙම ප්‍රවේශය බොහෝ ලෙස සුදුසු වනුයේ security assessment practices පිළිබඳ දැනුම ඔබගේ ආයතනයට අවශ්‍ය වූ විටක දීය.

කුමක්ද මේ Metasploit Framework ?

2003 වර්ෂයේ දී පමණ H.D. Moore විසින් open source project ලෙස Metasploit වැඩි දියුණු කළ අතර PERL මූලිකත්වයෙන් මුල් ආරම්භය සිදු වූ අතර 2007 වර්ෂයේ දී Ruby භාවිතාවෙන් එය නැවතත් hacker/ penetration tester community සඳහා ගැළපෙන පරිදි rewrote කිරීම ද Rapid7 මගින් developed කිරීම ද සිදු විය.
පසු කාලයේ දී Armitage නම් වූ ස්වාධීන developers ආධාරයෙන් free and open source GUI පරිසරයක් Metasploit ක්‍රියා කරවීම සඳහා පහත අයුරින් ඉතා සුන්දර හා ආකර්ෂණීය ලෙස නිර්මාණය කරන ලදී.

Metasploit භාවිතා කරනු ලබන්නේ පරීක්ෂා කිරීම සඳහා පමණක්ම අනවසරයෙන් පද්ධති තුලට ඇතුළුවීම (hacking into system) සඳහාය.

Metasploit සංස්කරණ විවිධ පරාස වල (Free, Professional or Enterprise editions) දකින්නට ලැබෙන අතර ඒ සියල්ල Metasploit Framework මත නිර්මාණය වේ. Quality-assured exploits එකතුවේ ඇති open source software development kit ලෙස මෙය ලොව තුල බහුතර පිරිසක් භාවිතා කරනු ලබයි.

මෙම Metasploit පහත පරිදි විවිධ ආරක්ෂක කටයුතු වලට භාවිතා කරනු ලැබේ.

- මෘදුකාංගවල ආරක්ෂාවට.
- තොරතුරු තාක්ෂණ වෘත්තිකයින්ගේ ආරක්ෂක ගැටලූ හඳුනා ගැනීමට.
- විද්වත් මත පදනම් කර සිදු කරනු ලබන ආරක්ෂක ඇඟයීම (vulnerability) සඳහා.
- ලිහිල් භාවය (mitigations) හඳුනා ගැනීමට.
- ආරක්ෂක ඇඟයීම් කළමනාකරණය කිරීමට.
- ස්මාර්ට් දුරකථන exploitation'
- මුර පදය විගණනය (auditing).
- වෙබ් යෙදුම් ස්කෑන් කිරීම් සහ සමාජ මෙහෙයවීම්. (social engineering)

මූලික නියමයන් තේරුම් ගැනීම (Understanding Basic Term)

Vulnerability - පද්ධතියේ ආරක්ෂාව පිළිබඳ යම් සම්මුතියක පැමිණීම නැතහොත් attacker කෙනෙකුට පද්ධතිය තුලට කඩා පැනීමට ඉඩ දීම වැනි දුර්වලතාවයන් මෙයට අයත් වේ.

vulnerable - පද්ධති පිළිබඳව යම් තොරතුරක් නැතිනම් වාසියක් ඇත්නම් ඒ ගැන ලිය ඇති codes ලබා ගැනීමට attacker වෙත ඉඩ සැලසීම මෙයට අයත් වේ.

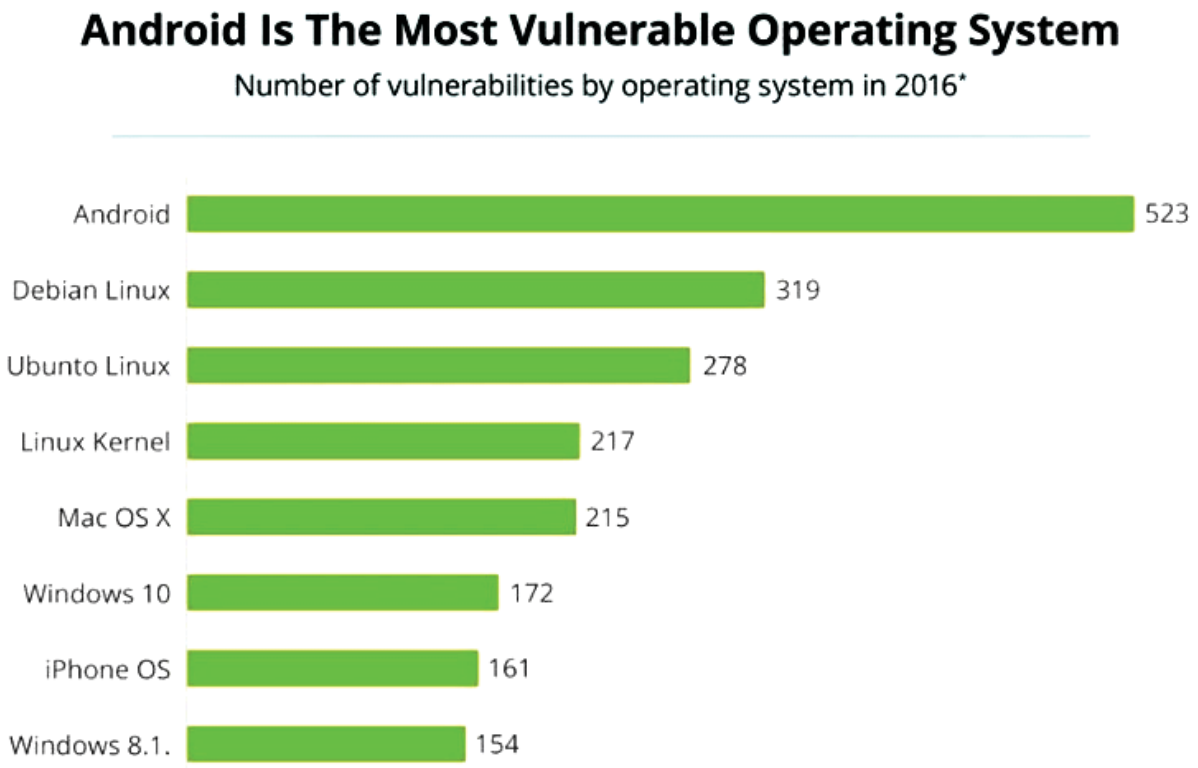
Payload - exploitation පසුව පද්ධතිය මත ධාවනය actual code මෙයට අයත් වේ.

Vulnerabilities ගැන දැන ගනිමු

ඔබගේ ආරක්ෂාකාරී ජාලට තුලට අනවසරයෙන් රිංගා ගන්නා මිනිසුන්, දත්ත, දෘශ්‍ය, මෘදුකාංග නිසා ඔබගේ වත්කම් වලට සිදු වන තර්ජනයන් හේතු කොට ගෙන ඒවා exploited කිරීමට සිදුවීම, ඒ පිළිබඳව vulnerabilities දැන ගැනීම ලෙස අර්ථ දැක්විය හැකි වේ. එනම් එම අරමුණු වෙනුවෙන් ඒවා exploit කරමින් මෙහෙයුම් පද්ධති හෝ යෙදුම් මෘදුකාංග වල දුර්වලතා සොයා බලා, මෘදුකාංගයන් පරීක්ෂාවට ලක් කිරීම මෙහිදී සිදු කරනු ලබයි.

Vulnerabilities පිළිබඳව අවබෝධ යක් ලබා ගැනීමට ඔබගේ ආරක්ෂා ව්‍යුහය (security structure) පිළිබඳ ඉගෙනීම කල යුතු වේ. තවද ඔබ හොදින් දන්නා වෙබ් අඩවි භාවිතා කර නව vulnerabilities පිළිබඳ තොරතුරු අන් අයට share කිරීම මගින් ඔබට සහ අන් අයට ද ජාල තුල ආරක්ෂාකාරී පසුබිමක් නිර්මාණය කර ගත හැකි වේ.

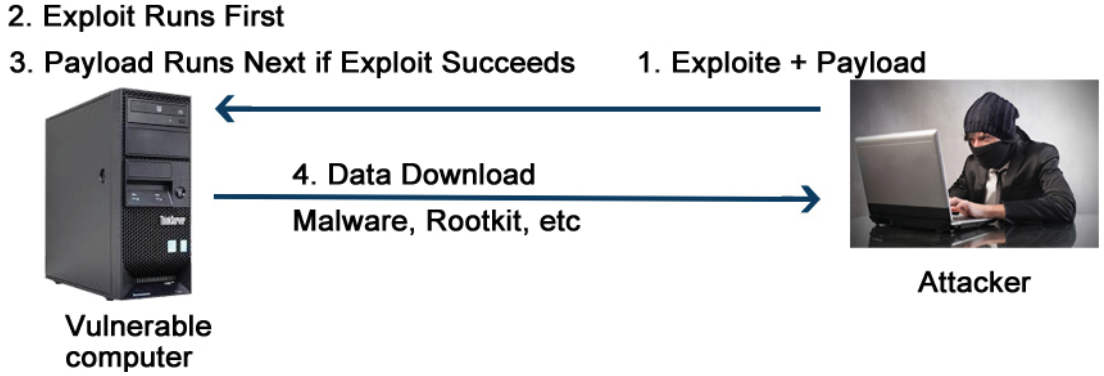
පහත පෙන්වා දී ඇති පරිදි Android මෙහෙයුම් පද්ධතිය සඳහා ඉහල ම vulnerability ලැබී ඇති අතර අවම අගයන් Microsoft Windows මෙහෙයුම් පද්ධති සඳහා ලැබී ඇත.



Exploitation ක්‍රියා කරන අයුරු

1. Vulnerabilities
2. Exploit
3. Payload

පහත පරිදි අංක පිළිවෙලට මෙම Exploitation සිදු වනු ලැබේ.



Exploiting යනුවෙන් මුලිකවම දැක්වෙන්නේ, යම් පද්ධතියක හෝ ජාලයක ඇති අනාරක්ෂිත ස්ථානයකින් ඇතුල් වීමෙන් තමාට අවශ්‍ය වන පරිදි වාසිය සාදා ගැනීමයි.

මෙම ක්‍රමය developed කර තිබෙනුයේ vulnerability භාවිතයේ ඇති වාසි දැන ගෙනය. එක් වරක් හෝ ඔබ vulnerability භාවිතයේ ඇති වාසි දන්නේ නම්, මෙය ඒ සදහා භාවිතයට ගත හැකි ලෙස දියුණු කර ගැනීමට හැකි වේ. මෙම කෘතිය තුල දී ඔබට එක් එක් අයුරින් සිදුවන attacks සහ නව exploits පිළිබඳව තොරතුරු අධ්‍යනය කල හැකි වේ.

තොරතුරු සොරා ගැනීමේ කලාව (ඔයැ ්රඒ දෙ ඊරැ්නසබට ෂබ)

1. Information Gathering

2. Scanning and Enumeration

3. Breaking in or Gaining Access

4. Privilege Escalation on the victim

5. Post Exploitation cleanup and Backdoor)ing

Penetration Testing Tools හඳුනා ගනිමු

1. Kali Linux

අද ලොව තුල තිබෙන digital forensics සහ penetration testing සඳහා ජනප්‍රියම මෙහෙයුම් පද්ධති අතරින් Kali Linux නැතහොත් Debian භාවිතයෙන් ව්‍යුත්පන්න කල Linux distribution එකකි. නොයෙකුත් විවිධ මානයන්ගෙන් සමන්විත වූ security and forensics ක්ෂේත්‍ර අවකාශය තුල මෙම Kali Linux මෙහෙයුම් පද්ධතියේ penetration testing වලට අදාල වන මෙවලම් 600 ක් තරම් විශාල ප්‍රමාණයක් අඩංගු වේ. වැඩිදුර අධ්‍යයනය සඳහා www.kali.org තුලට පිවිසීමෙන් ලබා ගත හැකි වේ. වර්තමානයේ දී Kali Linux 2017.1 සංස්කරණය ලෙස භාවිතා කරනු ලැබේ.

කුමක්ද මේ Debian

Debian නාමය මගින් ස්ථාවර, අස්ථායිතා, පරීක්ෂණ ත්තත්ව සහ පර්යේෂණාත්මක ශාඛා ඇති බව පැහැදිලි කරනු ලැබේ. Ian Murdock සහ ඔහුගේ බිරිඳ වන Debra විසින් 1996 දී මෙම Free මෙහෙයුම් පද්ධතිය සොයා ගෙන තිබේ. Ubuntu සහ වෙනත් බෙහෝ Linux මෙහෙයුම් පද්ධති නිර්මාණයට Debian මූලික වී ඇත.

2. Backtrack

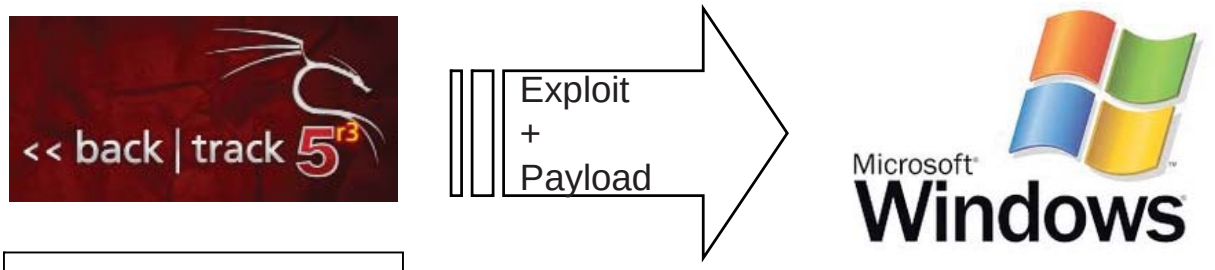
Backtrack යනු, Ubuntu GNU/ Linux distribution ඉලක්ක ගත කර ගනිමින් ඩිජිටල් forensics සහ penetration testing භාවිතා කිරීම ද පදනම් කර ගනිමින් තොරතුරු තාක්ෂණ ආරක්ෂක වෘත්තිකයින් සඳහාම නිර්මාණය කරන ලද මෙහෙයුම් පද්ධතියකි. තවද එය variety of software applications and tools වලින් සමන්විත වේ.

වර්තමානයේ දී Backtrack 5 R3 සංස්කරණය භාවිතා කරනු ලැබේ.

4

Microsoft Windows Attacks
හඳුනා ගනිමු

Microsoft Windows Operating System පද්ධතියට සිදුවන ප්‍රහාරයන් (Attacks) හඳුනා ගැනීම මෙහි දී සාකච්ඡා වනු ඇතී මෙහිදී එම කාර්යය සඳහා Metasploit Framework සහ meterpreter විධානයන් භාවිතයට ගනු ලබයී



Attacker System

Network Card in Bridge Mode

IP Address: 192.168.1.100

Victim/ Target System

Network Card in Bridge Mode

IP Address: 192.168.1.101

Metasploit Framework Console Commands (විධානයන්)

ඉහත පරිච්ඡේදය මගින් පැහැදිලි කල පරිදි Backtrack නම් මෙහෙයුම් පද්ධතිය ඔබ විසින් පරිගණකයට Virtual Machine භාවිතයෙන් ස්ථාපනය කර ඇතැයි මම විශ්වාස කරමි. ඉන්පසුව Metasploit නම් වූ මෙවලම් මෘදුකාංගය භාවිතයට ගනු ලැබේ. එය මෙහෙයුම් පද්ධතියට ඇතුල් කල පසු msfconsole නම් වූ console භාවිතයෙන් පහත පෙන්වා දී ඇති ලෙස backend commands ඇතුලත් කිරීම සිදු කරනු ලැබේ.

info - නිශ්චිත exploit හෝ module පිළිබඳ තොරතුරු ප්‍රවේශ කිරීම

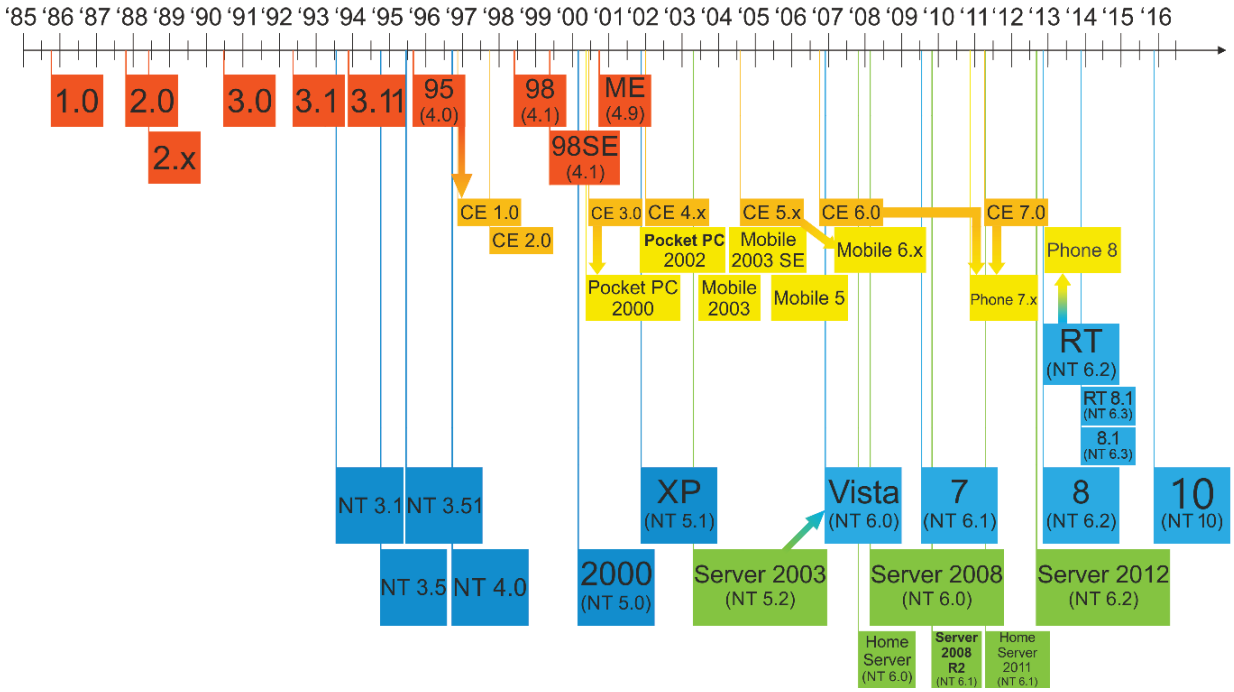
search name - Search for exploits or modules (msf > search pnp)

LHOST - ජාලය තුල ඔබගේ local IP address හෝ ඔබගේ ජාලයෙන් පිටත ඉල්කකයක් නම් එයට සම්බන්ධ public IP address

Microsoft මෙහෙයුම් පද්ධති වල Build No

ඔබගේ පරිගණකය තුලට යම් කිසි attack සිදුවනුයේ නම් එය පහත පෙන්වා දී ඇති පරිදි Microsoft Windows මෙහෙයුම් පද්ධති වලට අදාළ එහි Build අංකය පිළිබඳ පැහැදිලි දැනුමක් ඔබ සතුව තිබිය යුතු වේ.

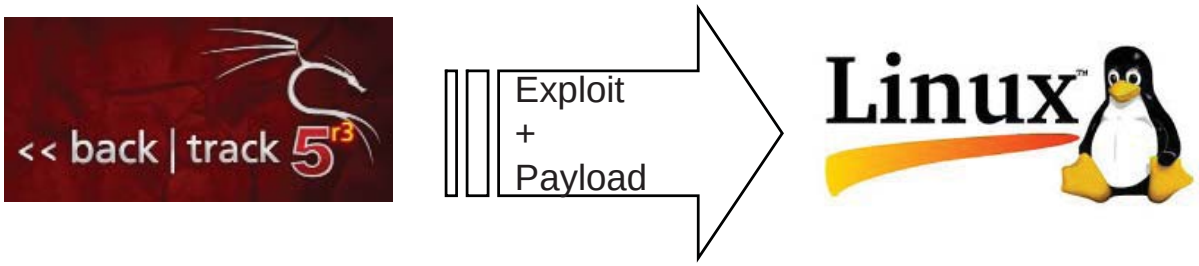
පහත ප්‍රස්ථාරය මගින් Microsoft Windows මෙහෙයුම් පද්ධති නිෂ්පාදනය කරන ලද වර්ෂය සහ ඊට අදාල වන Build අංකය පිළිබඳ තොරතුරු ලබා දෙනු ලැබේ.



Linux Exploitation හදුනා ගනිමු

5

Linux මෙහෙයුම් පද්ධතියේ Exploitation ක්‍රියාව



Attacker System

IP Address: 192.168.31.129

Target System

IP Address: 192.168.31.135

1. Backtrack 5 R2 Virtual Machine ට අදාල network card හි setting එක NAT mode පැවැත්විය යුතුවේ.

2. dhclient3 eth0 ලෙස Backtrack 5 R2 Machine අදාල IP Address අගයන් DCHP වල තබන්න.
3. Backtrack 5 R2 Machine ys IP address 192.168.31.129 ලෙස DHCP තත්ත්වයෙන් පවතී යැයි සිතන්න.
4. ඉලක්ක ගත Linux Virtual Machine හී ද network card ද NAT mode හි ම පවත්වා ගෙන යන්න.
5. dhclient3 eth0 ලෙස Linux Machine අදාල IP Address අගයන් DCHP වල තබන්න.
6. DHCP භාවිතයේ සිට 192.168.31.135 IP Address අගය Linux Machine හි තබන්න. එනම් Backtrack 5 R2 හි IP Address = 192.168.31.129 සහ Linux Machine හි IP Address = 192.168.31.135 ලෙස ය.
7. 192.168.31.135 ට Ping කිරීම සිදුකර පද්ධති දෙක අතර connectivity හොදින් පවතිනවාද පිරික්සන්න.
8. ඉලක්ක ගත Linux Virtual Machine හි run වන services, ඒවායේ versions සහ විවෘත වී තිබෙන ports මොනවා ද කියන දෑ සොයාගන්න.

6

Wireless Hacking හැඳින්වීම

පසුගිය වසර කිහිපය තුළ තොරතුරු පද්ධති සහ ජාල වල ආරක්ෂාව පිළිබඳ කථා කිරීම ඉතා උණුසුම් මාතෘකාවක් වී ඇත. කාලය වෙනස් වන අතර ඒ සම ම තාක්ෂණයේ දියුණුවත් සමග නව ප්‍රවේශ කරා යා හැකි අතර ඉන් එකකි 1998 වර්ෂයේ දී සොය ගනු ලැබූ Wi-Fi නොහොත් wireless local area networking නම් වූ රැහැන් රහිත ජාල නිර්මාණයයි.

අප පරිගණක සහ ඩිජිටල් යුගයක් තුල අප ජීවත් වන බැවින්, අලූත් ඉල්ලූමක් ඇති සේවා වන් වැඩි වෙමින් පවතින අතර සමාගම් බොහොමයක් ඔවුන්ගේ යටිතල ව්‍යුහය නැවත සකස් කර මෙම ඉල්ලූම සපුරාලීමට රැහැන් රහිත WLAN වැනි නව තාක්ෂණය බිහි කරනු ලැබේ. කෙසේ වෙතත්, සුපරීක්ෂාකාරී සැලසුම් නොමැති වීම (vulnerable system) අනතුරුදායක පද්ධතියකට මග පාදනු ඇත. තොරතුරු තාක්ෂණ වෙළඳපොළ තුල තාක්ෂණයේ නව වෙනසක් සිදු කරනු ලද්දේ නම් ඒ කිසිවක් නොව රැහැන් රහිත (Wireless) තාක්ෂණයයි. පසුගිය 15-20 වසර සඳහා Ethernet (Cabling) තාක්ෂණය භාවිතා වුවද මෙය එහි තාක්ෂණික පරිනාමණයයි. මෙහි ප්‍රතිඵලයක් ලෙස අප සියලූ දෙනා භාවිතා කරන පරිගණකල, ලැප්ටොප්, ටැබ්ලට් සහ ස්මාර්ට් ජංගම දුරකථන, ජංගම හා wire free තාක්ෂණය සඳහා අවශ්‍යතාව වැඩි වී ඇත.

ඉදිරි පිටු කිහිපය තුළ ඔබේ රැහැන් රහිත ජාලයේ WEP encryption සඳහා වූ vulnerabilities සෙවීමට අවධානය ලක් කිරීමට උත්සාහ කරන අතර Backtrack සහ AirCrack යන tools භාවිතා කරමින් WEP key ලබා ගැනීමට පියවරෙන් පියවර මාර්ගෝපදේශනයක් ලබා දෙනු ලැබේ. මෙම තොරතුරු භාවිතා කළ යුත්තේ ජාලය පරීක්ෂා කිරීමට පමණක් වන අතර නීති විරෝධී / සදාචාරාත්මක නොවන (any illegal / Non Ethical work) යටෙත් භාවිතා කිරීමට ඔබගේ පූර්ණ වගකීම දැක්විය යුතු වේ.

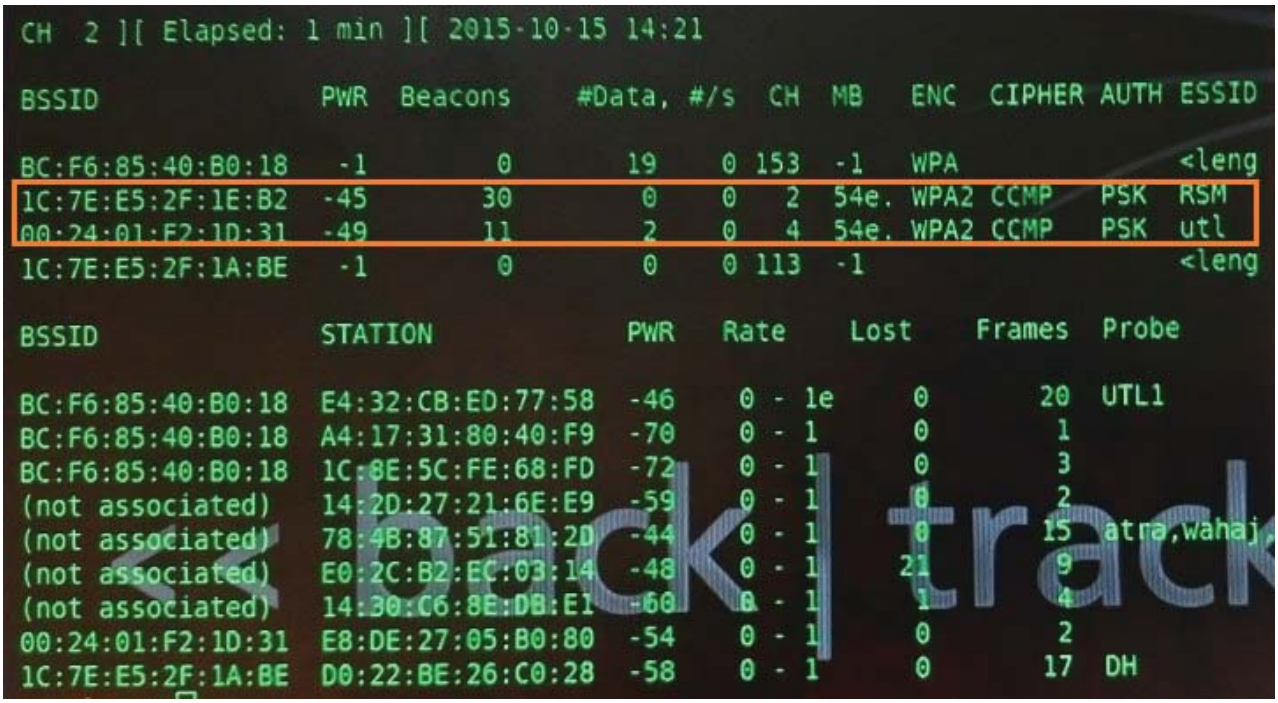
Aircrack-ng විධානය භාවිතා කරමු

මෙය packet detector නම් වූ application කී එසේම එය tool ලෙස WEP, WPA සහ WPA2 යන වර්ග වල රැහැන් රහිත 802.11 WLAN හරහා ගමන් කර ජාලය තුලට Attack සිදු කර password සොයා ඒවා Crack කිරීමට භාවිතා කරනු ලැබේ.

මෙම tool වර්ගය බොහෝදුරට යොදා ගනුයේ Linux (Kali distribution) මෙහෙයුම් පද්ධතියත් සමගයි

මීට අමතරව ඕනෑම රැහැන් රහිත ජාල අතුරු මුහුණතක පාලකය සමග ඒවා යේ driver supports raw monitoring mode සමග ක්‍රියා කරන අතර 802.11a, 802.11b සහ 802.11ට නම් වූ Wireless LAN සියල්ල sniff කිරීමට ද හැකියාව පවතී. මෙම වැඩසටහන Linux,FreeBSD, OS X, OpenBSD සහ Windows මෙහෙයුම් පද්ධති සමග ක්‍රියාත්මක වේ.

airodump-ng mon0 විධානය run කළ පසු එය පහත පරිදි දර්ශණය වනු ලැබේ. මෙහි දී රැහැන් රහිත ජාලය තුල RMS සහ UTL යන නම් වලින් හදුන්වා දිය හැකි Wi-Fi Routers දෙකක් දැකිය හැකි වේ



airodump-ng mon0 විධානය run කළ පසු එය පහත පරිදි දර්ශණය වනු ලැබේ. මෙහි දී රැහැන් රහිත ජාලය තුල RMS සහ UTL යන නම් වලින් හදුන්වා දිය හැකි Wi-Fi Routers දෙකක් දැකිය හැකි වේ.

Field	Description
BSSID	MAC address of the access point
PWR	Signal level reported by the card.
RXQ	Receive Quality as measured by the percentage of packets.
Beacons	Number of announcements packets sent by the AP.
CH	Channel number (taken from beacon packets).
MB	Maximum speed supported by the AP.
ENC	Encryption algorithm in use.
CIPHER	The cipher detected.
AUTH	The authentication protocol used.
ESSID	Shows the wireless network name.
STATION	MAC address of each associated station.

නිවස තුල පවතින රැහැන් රහිත ආරක්ෂාව (Home Wireless Security)

පහත පෙන්වා ඇති ක්‍රියාමාර්ග ගනිමින් රැහැන් රහිත නිවෙස් ජාලය ආරක්ෂා කිරීම සිදු කළ හැකි වේ.

- ඔබගේ wireless access point or router යේ ඇති default system ID වෙනස් කරන්න.
- ඔබගේ පද්ධතිය සඳහා පෙරනිමි මුර පදය (default password) වෙනස් කරන්න.
- Identifier broadcasting අක්‍රිය කරන්න.
- Encrypt wireless communications. (WPA - based encryption offers better protection than WEP-based encryption)
- Use your router's built-in firewall to restrict access to your network.
- ඔබේ රැහැන් රහිත පද්ධතිය ක්‍රමානුකූල ව යාවත්කාලීන ව තබන්න.

මහජන රැහැන් රහිත ආරක්ෂාව (Public Wireless Security)

පොදු ප්‍රවේශ ස්ථාන වල ඇති public access points (frequently called hotspots) වෙත සම්බන්ධ වීමට පෙර සලකා බැලිය යුතු පියවර පහත පරිදි විස්තර කරනු ලැබේ.

- හැකි නම් virtual private network (VPN) භාවිතා කරන්න.
- වෙබ් අඩවි වලට පුද්ගලික තොරතුරු ලබා දීම සහ passwords ලබා දීමෙන් වැලකී සිටින්න.
- Encrypt your files
- ඔබේ වටාපිටාව ගැන දැනුවත් වන්න.

7

විද්‍යුත් තැපැල් පණිවිඩ (E-mail) Hacking

E-mail යනු ඉතා පුළුල් ලෙස භාවිතා කරන සන්නිවේදනය සඳහා භාවිතා වන පොදු මෙවලමක් වන අතර එය වෙබ් අඩවි පදනම් කර ගනිමින් කොටස් දෙකකට වෙන කල හැකි වේ. එනම්, open සහ closed ලෙසය. විවෘත වෙබ් අඩවි පදනම් කර ගත් සේවාවෙන් ඕනෑම කෙනෙකු වෙත විද්‍යුත් තැපැල් ගිණුම් ලබා දෙනු ලබන්නේ නොමිලේ හෝ ගාස්තුවක් නොමැතිවය. Closed web-based services ආයතනයක සිටින සාමාජික-යන්ට පමණක් ලබා දෙනු ලබයි.

වාණිජ හා සමාජ වෙබ් අඩවි E-mail භාවිතා කරනුයේ එහි භාවිතය ආරක්ෂාකාරී නිසාය. E-mail ගිණුම hacked කිරීමට ඇති ප්‍රධාන හේතුව වන්නේ ඒවායේ අඩංගු පෞද්ගලික, සංවේදී හෝ රහසිගත තොරතුරු වෙත ප්‍රවේශ වීමට තිබෙන අවශ්‍යය. මෙය පරිශීලකයාට ඉතා හානිකර අතර සමහර වෙබ් අඩවි, බැංකු ගිණුම් සහ පෞද්ගලික ජීවිතයට තදින් ම බලපානු ලැබේ.

E-mail ගිණුමක hacked වීමක් සිදු විය හැකි අවස්ථා

Spam හරහා

අනවශ්‍ය වාණිජ හෝ තොග විද්‍යුත් තැපැල් (bulk E-mail) පණිවුඩ ප්‍රහාරකයන් විසින් පරිශීලකයාට ලැබීමට සැලැස්වීම මගින් Spam නිර්මාණය වීම සිදුවේ. සැගවුණු හෝ නොමග යවන IP ලිපිනය සහ සැගවුණු හෝ නොමග යවන E-mail address භාවිතයෙන් attackers නිතරම විශාල ලෙස E-mail විකාශන (broadcasts) සිදු කරනු ලැබේ. Spammer's පුද්ගලයින්ට ඔබ ආයතනයේ E-mail සහ IP address සඳහා ප්‍රවේශ වීමට ඉඩ තිබුණේ නම්, ඔබ සමාගමේ ව්‍යාපාරයට බලපෑම් සිදු කර එය විනාශකාරී තත්ත්වයට ඇද දැමිය හැකි වේ. එසේම එම E-mail සහ IP address සියල්ල blacklist ලැයිස්තුවට එකතු වී ඇති නම් අන්තර්ජාල සේවා සැපයුම්කරු (ISP) විසින් තවදුරටත් E-mail ගනු දෙනු සිදු නො කරනු ඇත.

වෛරසය (ඇසරම්) නිසා

වෛරසයක් ප්‍රවාහන මාර්ගයක් ලෙස විද්‍යුත් තැපෑල තුලට ඇතුළු වේ. මෙම වර්ගයේ වෛරස් බොහෝ විට අදරප ලෙස හැඳින්වේ. මෙම වෛරසය spamming framework රාමුවක් අකමැති තත්ත්වයක වුව ද පරිශීලකයාගේ පරිගණකය තුල නිර්මාණය කරයි. මෙය E-mail වල ආරක්ෂාවට ඉතා අන්තරාදායක මොහොතක් මක නිසා ද එමගින් spam දිගින් දිගටම ව්‍යාප්ත වී භයානක ඩසරම්ෑ ඇතුළු වීම සිදු විය හැකි නිසාය.

තතුබෑම් (Phishing) තුලින්

Phishing යනු සයිබර් ප්‍රහාරයක් වන අතර, පරිශීලකයා වෙතට සම්බන්ධ විය හැකි නීත්‍යනුකූල ව්‍යාපාර වලින් පෙනී සිටින විද්‍යුත් තැපැල් පණිවිඩ මෙයට ඇතුළත් වේ. මෙම Phishing ඊමේල් වංචාවක් වන්නා සේම ඔවුන් හිමිකම් කියනු ලබන්නේ ඔවුන්ගෙන් පැමිණෙන ලෙස පෙන්-වමින්ය. එසේම ගිණුම් අංකය, මුර පදය හෝ උපන් දිනය වැනි පෞද්ගලික තොරතුරු සනාථ කිරීම සඳහා මෙම පණිවුඩ ඔබගෙන් ඔබ නො දැනුවත් ම ඉල්ලා සිටී. 20% ක් වංචනිකයන් හට හසු වී ඔවුන්ට ප්‍රතිචාර දැක්වීමෙන්, සොරකම් කළ ගිණුම්, මූල්‍යමය පාඩුව හෝ අනන්‍යතා සොරකම් (identity theft) ඇති විය හැකී මෙම වර්ගයේ attacks පවතින නිසා අනවශ්‍ය විද්‍යුත් තැපැල් වලට ප්‍රතිචාර දැක්වීම සුදුසු නොවනු ඇත.

අනවශ්‍ය විද්‍යුත් තැපැල් ලිපිනයට ප්‍රතිචාර දැක්වීමට අවශ්‍ය යැයි සිතන්නේ නම්, ඒවා අනිසි ලෙස ක්‍රියා කිරීමක් ලෙස වැරදි ලෙස විනිශ්චය ගත කිරීම හෝ අමුතු වචන සඳහා පරීක්ෂා කිරීමට වග බලා ගන්න. එවැන්නක් විශ්වාස නොකරන ඊමේල් ඇමුණුම් විවෘත කිරීමට හොඳ අදහසක් නොවනු ඇත.

විද්‍යුත් තැපැල් සොරකම් (Hacking) පිළිබඳ සිද්ධීන්

නීති විරෝධී කටයුතු සඳහා Hacker වරුන් විසින් විද්‍යුත් තැපැල් පණිවුඩ හුවමාරු කර ගන්නා ඔබට වැදගත් අවස්ථාවන් පහත පෙන්වා දෙනු ලැබේ.

ABC නම් සමාගම, ඉලෙක්ට්‍රොනික භාණ්ඩ ආනයනය සිදු කරන ආයතනයකී රටවල් වලින් භාණ්ඩ ආනයනය කිරීම, ඇණවුම් තැබීම, ඇණවුම් සනාථ කිරීම (confirmation of orders), sending bank transfer receipts යැවීම වැනි කටයුතු සඳහා විද්‍යුත් තැපැල් සේවය අධික ලෙස භාවිතා කිරීම සිදු කරයි.

එක් දිනයක දී ABC ආයතනයේ sales department විසින් ඔවුන්ට SK Electronics ආයතනයෙන් ලැබුණු quotation අනුව එහි සේවය කරන Mr. Simon වෙත භාණ්ඩ මිල දී ගැනීම තහවුරු කරමින් යවන ලද E-mail පණිවුඩය පහත පෙන්වා දී ඇත.

From: ABC sales Dpt<sales@abccompany.com>
To: SK Electronics <simon@skelectronics.com>
Subject: Confirmation of order

This is to confirm that we will go ahead with the quotation you send us. Will make the necessary payment to usual bank account for the value of 25,000 USD

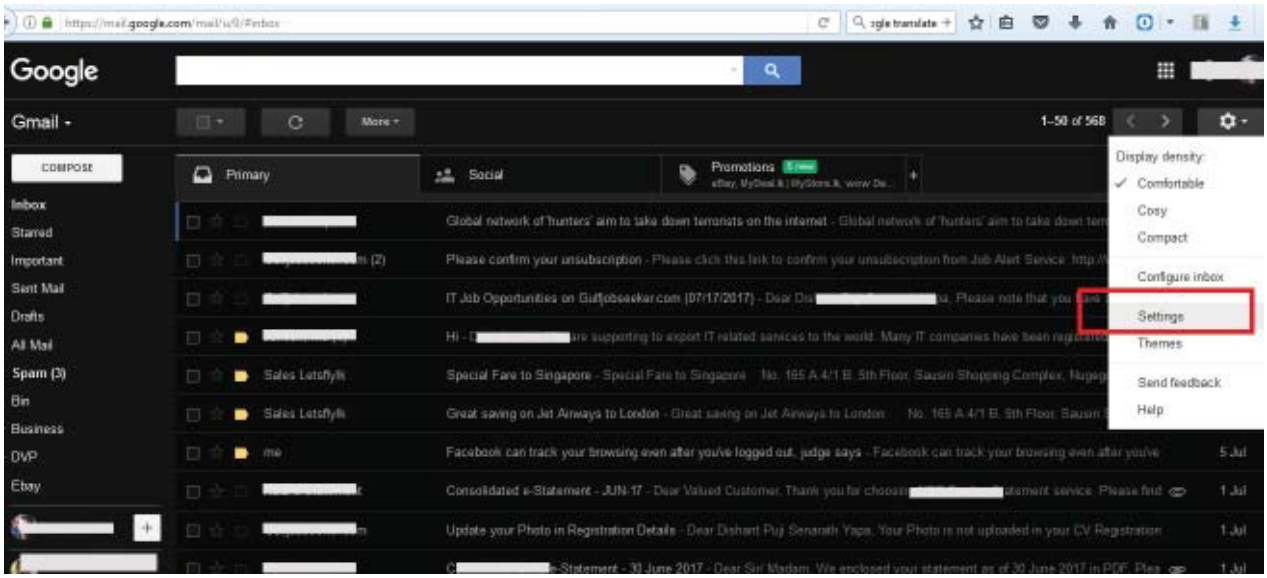
Thanks,
Ajith
Sales Department

විද්‍යුත් තැපැල් පණිවුඩ Hacker ගිණුමට හැරවීම (E-mail forwarding to hacker account)

ඔබගේ E-mail පණිවුඩ හොර රහසේම hacker විසින් ඔවුන් ගේ විද්‍යුත් තැපැල් ලිපිනයට (උදාහරණ. hacker@hacker.com) වෙත හරවා ගැනීම සිදු කල හැකි වේ. මෙම ක්‍රියාවලිය සිදු වී ඇති දැයි ඔබට ඔබගේ විද්‍යුත් තැපැල් ගිණුම තුල පහත පෙන්වා දී ඇති අයුරින් E-mail forwarding පිළිබඳව සොයා බැලිය සිදු කල යුතු වේ.

Gmail ගිණුම තුල Forwarding E-mail ලිපිනය සොයමු

Gmail ආයතනයට අයත් E-mail ලිපිනය-ක් ඔබ භාවිතා කරනුයේ නම්, පහත පරිදි Forwarding ලිපිනය කුමක්ද යන වග සොයා තැබීම ඉතා නුවනට හුරු වේ.



ඉහත රූපසටහනට අනුව ඔබගේ Gmail ගිණුමට අදාල වන දකුණුපස ඉහලින්ම පිහිටි දැති රෝදය මත click කරමින් setting තුලට ඇතුල්වන්න.

ඉන්පසු පහත අයුරින් Add a forwarding address මත click කරමින් එහි වෙනත් E-mail ලිපිනයක් තිබේ දැයි සොයා විමසන්න.

Facebook හැකර් යනු කවුරුන්ද?

8

අද වනවිට පරිගණක භාවිතා කරන පුද්ගලයින් අතරින් බොහෝ පිරිසක් Facebook සමාජ ජාල වෙබ් අඩවිය සමග සම්බන්ධ වී සිටී. නමුත් ඔවුන් බොහෝ දෙනෙක් තම පෞද්ගලික තොරතුරු අනවශ්‍ය පුද්ගලයින් අතට පත් වීම වැනි අපහසුතාව යන්ට ලක් වන අතර තම Facebook ගිණුම වෙනත් පුද්ගලයින්ගේ පරිපාලනයට නතු වීම නැතිනම් Hack වීම වැනි ගැටළුකාරී අවස්ථාවන්ට මුහුණාදීමට සිදුවේ.

මෙවන් අපහසුතාවයන්ට පත්වීමට බොහෝවිට හේතු වන්නේ Facebook වෙබ් අඩවිය තුල ඇති දෝෂ නොව තම Facebook ගිණුම තුල නිවැරදි ආරක්ෂක උපක්‍රම භාවිතා නොකිරීමය. ඔබේ Facebook ගිණුමේ ආරක්ෂාව ඉහල නංවා ගැනීම සඳහා අනුගමනය කළ හැකි සරළ උපක්‍රමයන් මෙම පරිච්ඡේදය තුලින් පෙන්වා දෙනු ලැබේ.

ශ්‍රී ලංකාව සිදු වන Cyber crimes

9

තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනයේ (ICTA) සන්නිවේදන අංශ-යේ ප්‍රධානී පවසන පරිදි, රජයේ විශාල ප්‍රමාණයක වෙබ් අඩවි මෙම cyber ප්‍රහාරවලට ගොදුරු වනුයේ ඒවා launch-ing කිරීමෙන් පසු එම වෙබ් අඩවි යාවත්කාලීන නො කර සිටීම නිසාය. ඒවා ට අවධාන යොමු කරනු ලබන්නේ පළමු මාස කීපයක පමණක් නිසා එම වෙබ් අඩවි පහසුවෙන් ම hacker කරුවන්ගේ ගොදුරු බවට පත් වේ.

තවදුරටත් ඔහු පැවසූ පරිදි රජයේ ආයතන වලට cyber security පිළිබඳ දැනුවත් කරනු ලබන අතර එම ආයතන වල වගකීම වනු යේ ආයතනයේ ප්‍රතිරූපය රැක ගනිමින් එම hacker කරුවන්ගෙන් ඔවුන්ගේ වෙබ් අඩවි ආරක්ෂා කර ගැනීමය. දුර්වල ලෙස developed applications සහ වෙබ් අඩවි major vulnerability සඳහා අවස්ථාව සපුරා ගනු ලැබීම මෙහි දී සිදු වේ.

ශ්‍රී ලංකා තුල hacker ප්‍රහාර වලට ලක්වූ වෙබ් අඩවි

මෙම 2017 වර්ෂයේ ආරම්භයේ සිට පහත වෙබ් අඩවි hacker ප්‍රහාර වලට භාජනය වී තිබේ

අධිකරණ අමාත්‍යාංශය (Justice Ministry)
සේවක අර්ථ සාධක අරමුදල (Employees Provident Fund)
ජාතික කෞතුකාගාරය (National Museum)
ආගමන විගමන දෙපාර්තමේන්තුව (Immigration Department)
කෘෂිකර්ම දෙපාර්තමේන්තුව (Agriculture Department)
පරිවාස දෙපාර්තමේන්තුව (Probation Department)
ඌව පලාත් සංචාරක අංශය (Uva Province Tourism division)
උපාය මාර්ගික ව්‍යවසාය කළමනාකරණ ආයතනය - Strategic Enterprise Management Agency (SEMA)
ජාතික ආරක්ෂාව පිළිබඳ මාධ්‍යය මධ්‍යස්ථානය - Media Centre for National Security (MCNS)
උතුරු මැද පළාත් සභාව (North Central Provincial Council)
වරාය අධිකාරිය (Ports Authority)
ආයෝජන මණ්ඩලය (Board of Investment)
නෙළුම් පොකුණ ර හල් වෙබ් අඩවිය (Nelum Pokuna Theatre)
ක්‍රීඩා අමාත්‍යංශය (Ports Minister)
ලංකා රූපවාහිනී සංස්ථා වෙබ් අඩවිය (Rupavahini Sri Lanka television channel)
විදේශ කටයුතු අමාත්‍යංශය (Foreign Employment Bureau)
ශ්‍රී ලංකා රේගුව (Sri Lanka Customs)
විදුලි සංදේශ නියාම කොමිසම (Telecommunication Regulation Commission)
තක්සේරු දෙපාර්තමේන්තුව (Valuation Department)
මුදල් කොමිෂන් සභාව (Finance Commission)
වෛද්‍ය පර්යේෂණ ආයතනය (Medical Research Institute)

පහත දැක්වෙන පරිදි 2016 වර්ෂයේ දී පාසල් සිසුවෙකු විසින් ජනාධිපති නිල වෙබ් අඩවිය වන www.president.gov.k ද hacker කරුවන්ගේ සයිබර් ප්‍රහාරයට ලක් විය.

එසේම ආසියානු කලාපයේ සිටින hacker කරුවන්ගේ සයිබර් ප්‍රහාර වලට ශ්‍රී ලාංකික වෙබ් අඩවි 129 ක් පමණ ගොදුරු විය. Computer Emergency Response Team Co-ordination Centre (CERT|CC) ආයතනය පවසන පරිදි ශ්‍රී ලංකාව ඉදිරියේ දී අසමතුලිත නිවාරණ විධික්‍රම සහ පෞද්ගලිකත්ව නීති නොගැළපීම් නිසා massive wave of cyber attacks සිදු විය හැකි වේ. තවද CERT ප්‍රධානී පවසන පරිදි ශ්‍රී ලංකාව තුල සිදුවන major attacks තවමත් ප්‍රධාන සිරස්තල නොවුනත් එය ඉදිරි අනාගතයේ දී සිදු වනු ඇති බවද 2007 වසරේ සිට පරිගණක අපරාධ පනත ක්‍රියාත්මක වනු ලබන බවද පැවසීය.

10

ලොව පුරා සිදු වන සයිබර් ප්‍රහාර (Global Cyber-attacks)

සයිබර් ප්‍රහාරයක් යනු හිතා තාම පරිගණක ජාලයක ඇති තොරතුරු වෙනස් කිරීම, අවුල් කිරීම හෝ විනාශ කිරීමයි එවැනි ප්‍රහාර එල්ල කිරීම සිදු කරනු ලබනු යේ පරිගණක ගැන ඉහල දැනුමක් ඇති පුද්ගලයන් නැතිනම් Hacker ලා විසින්ය.

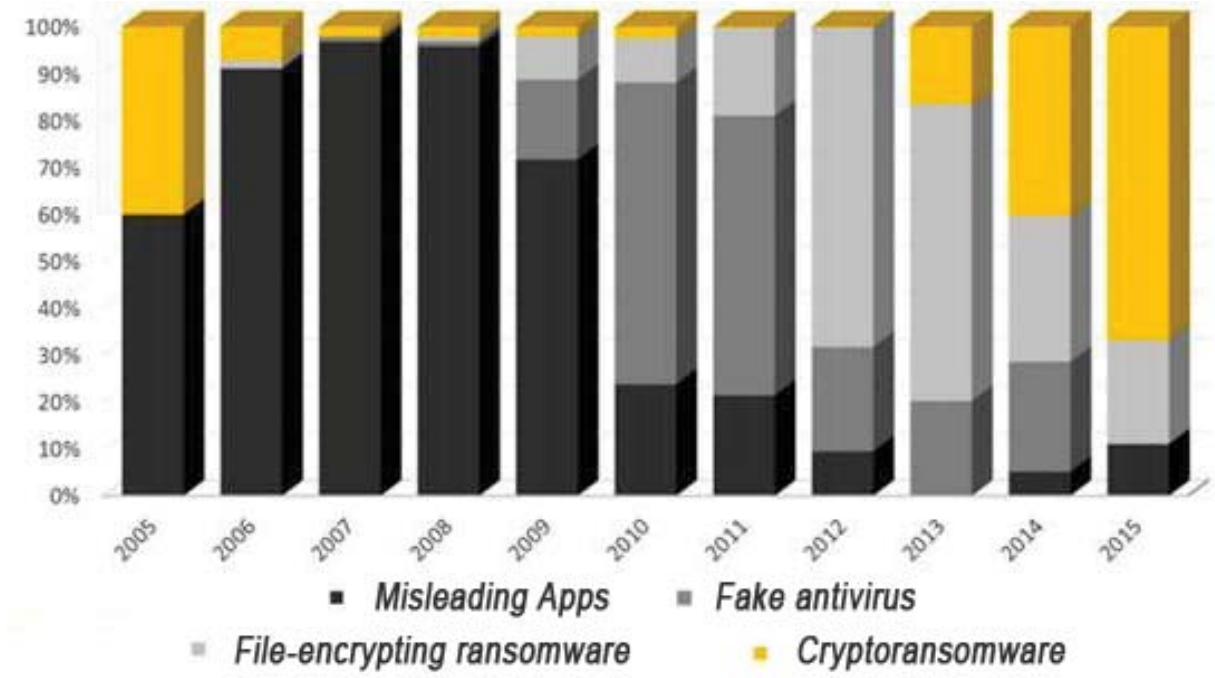
ඔවුන් අයථා ලෙස වෙනත් අයගේ පරිගණක තුළට ඇතුළු වී එහි ඇති තොරතුරු තම පාලනයට නතු කර ගෙන එම රටේ තිබෙන සියලු අන්තර්ජාලය මගින් සිදු වන සේවාවන් අඩාල කිරීමට හැකියාව තිබේ. ඔවුන් විකාශනය කරන හානිකර පරිගණක කේතයන් මගින් විනාඩි කිහිප-යක් ඇතුළත එම රටේ යුධ මෙහෙයුම්, මූල්‍යමය සහ ව්‍යාපාරික තොරතුරු ඇතුළත් ජාලවල ක්‍රියාකාරිත්වය අඩාල කිරීම සිදු කරනු ලබයි. තවද බැංකු ක්ෂේත්‍රයේ ටේලර් යන්ත්‍ර හා දුරකථන පද්ධති මුළුමනින් අඩාල වෙයි ගුවන් ගමන් සහ න්‍යෂ්ටික බලාගාරවල ආරක්ෂාව සඳහා ඇති පරිගණක පද්ධති පවා ඇනහිටිය හැකි වේ.

මිනිසුන් මෙවැනි සයිබර් ප්‍රහාර එල්ල කිරීමට පෙලඹෙන්නේ ඇයි? ඔවුන් එය කරනු ලබන්නේ කෙසේ ද?

ඔවුන් එක් එක් පුද්ගලයන් ව ඉලක්ක කර ගෙන ප්‍රහාර එල්ල කරන නිසා ඔබට ඉන් ආරක්ෂා විය හැක්කේ කෙසේ ද? විවිධ හේතු නිසා පුද්ගලයන් සයිබර් ප්‍රහාර එල්ල කරයි. ත්‍රස්තවාදීන් විසින් ඔවුන්ට එදිරිවාදී වූ යම් රජයක් තුල වූ පරිගණක ජාලවලට ඇතුල් වී රහස් තොරතුරු හෝ යුධ උපකරණ පිළිබඳ තොරතුරු සොරා ගැනීමට හෝ ඒවාට හානි කිරීමට මෙම උපක්‍රමය යොදා ගනු ලබයි.

රැන්සම්වෙයා වැඩසටහනක් පරිගණකයට විත් තැන්පත් වන්නේ සාමාන්‍ය වයිරස් වැඩසටහනක් මෙනී ඉන්පසුව එය සාමාන්‍ය විදියට හදුනාගත නොහැකි වන පරිදි පරිගණකයේ සාමාන්‍ය ෆයිල් එකක වෙස් ගනී ට්‍රොජන් වැඩසටහනක් මෙනී එතැන් පටන් පරිගණකය අක්‍රීය කරමින් කප්පම් ඉල්ලයී මීටත් අමතරව mobile සඳහා ද ransomware ප්‍රහාර සිදුවී ඇති එහිදී Android මෙහෙයුම් පද්ධතිය ප්‍රධාන ගොදුර බවට පතිවී තිබේ

පහත ප්‍රස්ථාර මගින් ransomware වලින් සිදුවී ඇති ප්‍රහාර පිළිබඳ අවබෝධය ලබා දෙනු ඇති



පහත අයුරින් decrypt key කප්පම් මුදල ගෙවා ලබා ගත යුතු වේ

Ransomware threats spread වී මේ විවිධ ක්‍රම

සරලම ක්‍රමය නම් ව්‍යාජ නමුත් සැබෑ ලෙස පෙනෙන අවවාදාත්මක පණිවුඩ එවීමය. පරිගණකයේ අසැබි දේ තිබේය කියා ආරක්ෂක අංශ විසින් එවන්නාක් සේ පෙනෙන පණිවුඩ එවීමයි. අනවසර මෘදුකාංග පරිගණකයේ තිබේය කියා පණිවුඩ එවීමද දක්නට හැක. මෙහිදී දින වකවානුවක් දෙනු ලැබේ. එදිනට කලින් ඉල්ලන කප්පම් මුදල නොගෙවිවොත් පරිගණකය අකර්මන්‍ය කරන්නේ යැයි හැකර්කරුවා කියයි. මීට වඩා තරමක් අසීරු අවස්ථාව වන්නේ පරිගණකය අක්‍රීය කරන රැන්සම්වෙයා ඇති විටය.

එවිට මුලින්ම පරිගණකය අක්‍රීය (lock or restrict) කරයි. දැන් යථා තත්වයට ගෙන දෙන්නට කප්පම් ඉල්ලයි. නරකම විදිය වන්නේ, රැන්සම්වෙයා වැඩසටහන මගින් පරිගණකයේ අත්‍යවශ්‍ය file එන්ක්‍රිප්ට් කිරීමය. විශේෂයෙන්ම Hard disk ඇති system files එන්ක්‍රිප්ට් (Crypto viral Extortion) කිරීමය. මෙය යථා තත්වයට ගෙන එන්නට කිසිම විශේෂඥයෙක්ට ද නොහැකිය. කළ යුතු එකම දෙය රැන්සම්වෙයා වැඩසටහන නිර්මාණය කළ තැනැත්තා පමණක් දන්නා යථාවත් කිරීමේ කේතය (encryption key) ලබා ගැනීම පමණි. එතනදී කප්පම ගෙවිය යුතුය.

පහත Microsoft මෙහෙයුම් පද්ධති වලට පසුගිය කාලය තුලදී මෙම Ransomware Worm Attack - WannaCry ප්‍රහාරය එල්ල වී ඇත. එසේම එම Microsoft ආයතනය විසින් මෙම අවධානම සඳහා 2017 වර්ෂයේ මාර්තු 14 වන දින Microsoft Security Bulletin MS17-010 නමින් security patch එම පරිගණක යාවත්කාලීන කර ගැනීම සඳහා නිකුත් කරන ලදී.

- Windows Vista (සියලු editions)
- Windows Server 2008 (සියලු editions)
- Windows 7 (සියලු editions)
- Windows Server 2008 R2 (සියලු editions)
- Windows 8’1 (සියලු editions)
- Windows RT 8’1 (සියලු editions)
- Windows Server 2012 and Windows Server 2012 R2 (සියලු editions)
- Windows 10 (සියලු editions)
- Windows Server 2016 (සියලු editions)

ලොව පුරා සිදු වන සයිබර් ප්‍රහාර Online බලමු

ලොව පුරා විසිරුණු Hacker ප්‍රහාර කරුවන් ගේ තොරතුරු සජීවීව (on-line) Cyber Attack Maps ලෙස ඔබට ලබා දීම පහත දැක්වෙන වෙබ් අඩවි හරහා ලබා දෙනු ලැබේ

ී Norse`s map නම් වූ මෙය භාවිතයෙන් the country of attack origin, attack type, attack target country and displays a live feed of attacks ලබා දෙනු ලැබේ තවද location and by protocol අනුව එම දත්ත පිරික්සීමට ද පුළුවනී

http://map.norsecorp.com

Check Point නම් මෙම වැඩසටහන මගින් Hacker ප්‍රහාරකයන් සහ ප්‍රහාරයට ලක් වන රට වල් වල තොරතුරු ද ඊට අමතරව දිනය තුල ඇතිවූ attacks ප්‍රමාණය ද සොයා හැකි වේ. පහත සිතියම අනුව අද දින සිදු වූ attacks ප්‍රමාණය මිලියන 2.6 කට වඩා වැඩි අගයක් ගනු ලැබේ.

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

ශ්‍රී ලංකාව තුල 2017 ජුනි මස 22 දින සිදු වුන attack පිළිබඳ විස්තරය පහත පෙන්වා ඇත.