ШИНЖЛЭХ УХААН ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
Мэдээлэл холбооны технологийн сургууль

ЛАБОРАТОРИЙН АЖЛЫН ТАЙЛАН

Мэдээллийн аюулгүй байдал (F.NSN231)
2023-2024 оны хичээлийн жил
намар

Лабораторийн ажлын дугаар, нэр:	**Лаб-9, Адилтган танилт болон хандалтын удирдлагын ойлголтууд**
Хичээл заасан багш:	Х.Уянгаа /J.ES07/
Лабораторийн ажил гүйцэтгэсэн:	Оюутан: О.Уянга /B221870006/

Авбал зохих нийт оноо:	**1 оноо**	
Гүйцэтгэлийн шалгуур	**Үнэлгээний эзлэх хувь**	**Багшийн үнэлгээ**
Үндсэн гүйцэтгэл	70%	
Хавсарга гүйцэтгэл	10%	
Бичиглэл, найруулга	10%	
Хамгаалсан байдал	10%	
Нийт үнэлгээ	**100%**	
Хамгаалсан огноо		

2023-11-05

I. Тойм

Энэхүү лабораторийн ажлын зорилго нь лекцийн хичээлээр судалсан адилтган танилт болон хандалтын удирдлагын ойлголтуудын талаарх мэдлэгээ бататгах болон тэдгээр ойлголттой холбоотой аюулгүй байдлын сэтгэлгээг хөгжүүлэх даалгавруудыг гүйцэтгэх юм.

II. Гарчиг

III. Үндсэн гүйцэтгэл

A. Даалгавар 1:

Дараах үгнүүдийг нууц үг болгон ашиглахад тохиромжтой эсэхийг тодорхойлж, шалтгааныг тайлбарлана уу?

(a) YK 334 – Сул нууц үг. Үсэг тооны урт хэт богино.

(b) mfmitm (“my favorite movie is tender mercies”-ын товчлол)-Хүчирхэг нууц үг байж болох ч энэ товчлолыг өөр хүн мэддэг бол хүчингүй.

(c) Natalie1-Дунд зэргийн сул нууц үг.

(d) Washington- Сул нууц үг. Тоо тэмдэг ашиглаагүй түгээмэл нэршилтэй.

(e) Aristotle-Сул нууц үг. Нарийн төвөгтэй бус нийтлэг.

(f) tv9stove - Дунд зэргийн сул нууц үг. Тоо үсгийг хамтатган ашигласан.

(g) 12345678-Сул нууц үг. Дараалалсан тооноос бүрдсэн хамгийн нийтлэг сул нууц үг

(h) Dribgib-Дунд зэргийн сул нууц үг. Үсэг холин бичсэн.

B. Даалгавар 2:

Нууц үг нь ихэвчлэн таны мэдэж буй зүйл дээр үндэслэсэн үнэмлэх гэж тооцогддог. Тэгвэл

(a) Нууц үгийг бичиж тэмдэглэж авсны дараа таны мэдэж буй зүйл дээр үндэслэсэн үнэмлэх хэвээр байх уу? Тийм бол яагаад? Үгүй бол яагаад?

- Нэвтрэх үйл явц нь мэдлэгт суурилсан хэвээр байгаа хэдий ч зөвшөөрөлгүй нэвтрэх эрсдэл нэмэгддэг тул нууц үг бичихийг эсэргүүцдэг.

(b) Яагаад нууц үгийг бичиж авалгүйгээр цээжлэхийг зөвлөдөг вэ?

- Өөрт санахад хялбар тоо үсэг тэмдэгт хольсон нийтлэг бус нууц үг сонгох хэрэгтэй. Нарийн төвөгтэй санах шижүүргүй нууц үг зохиосноор дахин санахад төвөгтэй болдог. Түүнийг тэмдэглэж авах болох веб броувсер дээр хадгалан үлдээснээр бусдад нууц үгээ хурдан алдах эрсдэл үүснэ.

(c) Хэрвээ дээрх “нууц үгийг цээжлэх нь зүйтэй” гэсэн зөвлөмжтэй санал нийлэхгүй байгаа бол өөр ямар арга ашиглаж болох вэ? Тэдгээр аргуудад аюулгүй байдлын ямар асуудлууд тулгарч болох вэ?

-Нууц үгийг цээжлэхгүйгээр хадгалах аргад:

- Веб броусер дээр хадгалж үлдээх-
- Тухайн төхөөрөмжний note хэсэгт тэмдэглэн үлдээх-
- Биометрик хэрэглэгдэхүүн ашиглан шууд нэвтэрдэг болгох-
- Цаасан дээр бичин наах-

C. Даалгавар 4:

Нууц үг нь 26 тэмдэгтийн хэрэглээгээр хязгаарлагдах ба 4 тэмдэгтийн урттай байна гэж үзье. Мөн халдлага үйлдэгч секунд тутамд нэг нууц үгийг таахыг оролддог чадамжтай байг гэж үзье. Тэгвэл

(a) Нууц үгийн боломжит бүх хувилбарыг шалгаж үзэх дуусах хүртэл халдлага үйлдэгчид ямар нэгэн хариу өгөхгүй тохиолдолд зөв нууц үгийг олох хүртэл ямар хугацаа шаардагдах вэ?

- $26^4 = 456{,}976$ секунд. Үүнийг цаг руу шилжүүлэн бодвол $\frac{456{,}976 \text{ секунд}}{60*60} \sim 126.94$ цаг буюу ойролцоогоор 127 цагийг бүх хослолыг туршиж үзээд зөв нууц үгийг олоход зарцуулна.

(b) Буруу тэмдэгт оруулах бүрд халдлага үйлдэгчид алдааны мэдэгдэл өгдөг бол зөв нууц үгийг олох хүртэл ямар хугацаа шаардагдах вэ?

- Хэрэв халдагчид секунд тутамд нэг нууц үг таах боломжтой бол энэ тохиолдолд зөв нууц үгийг олоход 26*4=104 секунд шаардлагатай.

IV. Дүгнэлт

Адилтган танилт болон хандалтын удирдлагын ойлголтуудын талаарх мэдлэгээ бататгасан.

V. Ашигласан материал

[1] F.NS251: Мэдээллийн аюулгүй байдлын үндэс, Лекц-7
[2] F.NS251: Мэдээллийн аюулгүй байдлын үндэс, Лекц-8
[3] Shon Harris, Fernando Maymí. "CISSP All-in-One Exam Guide", 8th Edition, 2018, Chapter 3,5
[4] William Stallings, Lawrie Brown "Computer Security: Principles and Practice", 4th Edition, 2018, Chapter 3, 4