1. SQL-injection – går det att skydda sig?

Christoffer Söderlund, Linus Göransson

Idag är de flesta hemsidor kopplade till någon sorts databas. I vårt projekt kommer vi att testa hur SQL-injections fungerar i dagsläget. SQL-injection är ett sätt att manipulera hanteringen av indata som arbetar mot en databas för att till exempel få obehörig tillgång till ett system. Hur användbart är det? Kan man förbättra säkerheten emot det? Går det att skydda sig helt emot det?

2. Lösenordsanalys - Hur bygger vi starka lösenord och minns dem?

Emil Hjertsson, Henrik Lennart Kentsson

Vårt projekt handlar om att analysera lösenord uppbyggda på olika vis och genomföra lösenordsknäckning på de hashsummor som skapas utifrån dessa. Detta gör vi för att ta reda på vad det är som gör ett lösenord starkt eller svagt. Lösenord skall även vara möjliga att minnas så vi tar upp olika metoder för hur man kan skapa lösenord som är starka och samtidigt enkla att minnas.

3. Analys och jämföring av wipeverktyg

Christoffer Kindberg, Jonas Fredrik Kurkinen

Projektet handlar om att vi ska testa olika wipeverktyg, i jämförelsen ska vi tänka på vilket verktyg som är bäst i kategorier som användarvänlighet, pris, prestanda och vad verktyget kan erbjuda beroende på vilken prisklass man arbetar i. Vi ska testa dessa wipeverktyg på en hårddisk som vi efter varje wipe och analys klonar med vår originaldisk så vi alltid får tillbaka vår originaldata så vi får ett jämnt resultat om verktyget fungerar och om något inte fungerar så ser vi vad som gick fel. Vi valde detta projekt för att vi vill upplysa allmänheten om att man lätt kan wipa sin hårddisk och att man borde göra det innan man gör sig av med den (sälj, släng, byter).

6. USB-Attacker och skydd

Robert Denham-Smith, Tommy Berggren

Syftet med vårt arbete är att via befintlig litteratur, försöka kartlägga huruvida det finns negativa aspekter av USB-enheter och i så fall vad man måste ta hänsyn till när man brukar en potentielt infekterad enhet. Närmare bestämt vilka svagheter i operativsystemet som kan utnyttjas och vad man kan göra åt dessa. Ett av våra primära mål med uppsatsen är att försöka förmedla kunskap om potentiella risker till den ”vanlige” användaren, som kanske inte besitter större IT-kunskaper. Man skulle kunna kalla det en slags säkerhetspolicy för användning av USB-enheter.

7. Steganografi i digital miljö

Emil Heehrle, Patrik Dahlgren

Användning av steganografi för att gömma data. Test av steganografimjukvaruprogram. Analys av carrierfiler, undersökning om det går att upptäcka gömd data.

8. ???

Patrik Barkstedt, Sandro Bizzarri

????

9. Sårbarheter i trådlösa nätverk, Wi-Fi Protected Setup (WPS)

Thimmy Eklund, Peter Eliasson, Marcus Hansson

Projektet kommer kortfattat beskriva hur WPS fungerar samt demonstrera sårbarheten som upptäcktes i december 2011. Sårbarheten gör det möjligt att kringgå en stark WPA/WPA2-kryptering genom att attackera WPS PIN-kod med en brute force attack.

10. -Wireshark- Displayfiltrets grundläggande egenskaper

Jim Persson, Magdalena Rosenberg

Analys av nätverkstrafik kräver ett tränat öga och kunskap om hur inspelad trafik kan hanteras, filtreras och sorteras. Längre inspelningar eller intensiv nätverksaktivitet kan resultera i en stor mängd paket och den information du letar efter försvinner lätt.Vi kommer göra en kortfattad presentation över displayfiltret i Wireshark och ge några exempel på nätverksattacker samt relaterade filter.

11. SSL sårbarheter

Anton Dahlqvist, Peter Sjöholm

Vi tar reda på om SSL en tillräckligt bra teknik för att användas vid känsliga Internet-aktiviteter?Vi förklarar hur SSLstrip fungerar och genomförs i en attack samt hur man kan skydda sig mot dessa typer av attacker.Där vi även kommer att visa exempel på hur vi gjorde för att få inloggningsuppgifter till olika https sessioner, som banker, facebook och gmail.

12. Den elaka tvillingen

Jan Fredrik Johansson, Jörgen Johansson, Lars Marcus Johansson

Hur farligt är det att ansluta sig till trådlösa nätverk med fokus på den elaka tvillingen.

13. Android – Forensisk avbild, databasanalys, GPS utvinning och automatisering med Python

Christelle Kellgren, Martin Fransén

Hur skapar man en forensisk avbild av Android? Vilka spår lämnas i databaserna när du surfar på din Android-telefon eller när du får ett inkommande sms? Geo-taggade bilder, filerna cache.wifi och cache.cell lämnar geografiska avtryck. Hur kan vi utifrån den geografiska datan kartlägga platserna med hjälp av Google Earth?

14. Gömda program - hur malware gömmer sig med hjälp av rootkits

Oliver Ohlsson, Martin Svedhage, Philip Teveldal

Vi berättar om vad malware är för något och förklarar sedan hur de gömmer sig med hjälp av rootkit samt vad ett rootkit är för något. Vi har också ett mindre experiment med en keylogger

15. Keyloggers - Dess funktionalitet och enkla säkerhetsåtgärder

Marcus Larsson, Tina Gustavsson

Vi kommer granska begreppet keylogger för att försöka förklara vad en keylogger är samt hur den kan användas i en datormiljö. Vi kommer också resonera kring de etiska aspekterna angående användning av keyloggers i hemmiljö och på arbetsplatsen samt hur det ser ut rent juridiskt. Vi kommer även utföra tester på ett antal olika keyloggers för att ge svar på hur programmen kan användas, hur dom går att dölja för den utsatte användaren och dess funktionalitet samt ge råd hur man som användare kan gå tillväga för att minska riskerna att få viktig information loggad.

16. ???

Henrik Ryttergard, Livia Klemens

???

17. Granskning av sårbarheter i Windows Server - Före och efter härdning

Mats Engman, Niklas Åqvist

Vi kommer i vårt projektarbete att undersöka vilkapotentiella sårbarheter som finns i en nyinstalleradWindows Server 2008 R2, och därefter installera de senaste uppdateringarna samt genomföra engrundläggande härdningsprocess. Efteråt kommer vi att utföra en till sårbarhetsanalysoch jämföra resultaten före och efter.

18. Analys av säkerheten hos trådlösa datanätverk

Erman Bostanci, Karl Robert Brorsson

Hur säkra är de krypteringstekniker som används i våra moderna trådlösa datanätverk? Det är vad vi har försökt ta reda på i vårt projekt. Vi har utfört test och analys och utifrån detta skall vi försöka ge en bild av hur bra dessa är.

19. Steganografi och Stegoanalys av JPEG och BMP

Alexander Svensson, Markus Svensson

Steganografi handlar om att gömma hemlig eller känslig information som bilder eller texter helt synligt. Det man vill är att få det gömda att framstå som något helt oskyldigt, som t.ex. en tabell, artikel, shoppinglista, eller en bild. I dagens digitaliserade värld har konsten att steganografera blivit tillgänglig för gemene man med tillgång till en dator och ämnet blir bara större och större och därför är steganografi och stegoanalys bra för en IT-forensiker att kunna. I detta arbete behandlar vi hur JPEG och BMP påverkas av steganografering och hur man kan upptäcka detta med hjälp av stegoanalys.

20. Att bygga ett steganografi-program

David Johansson, Michael Dubell

Vi har byggt ett litet steganografi-program i programmeringsspråket Python. Programmet använder sig LSB-tekniken(Least Significant Bit) och kan gömma meddelanden i PNG bilder och även återskapa det gömda meddelandet

från stego-bilder som skapats med programmet.

21. Moderna virus: från poesi till cyberspionage

Bonnie Malmström, Louise Kadre

Vi börjar med att redogöra för några vanliga typer av malware och berättar kort om virusens utveckling de senaste decennierna. Därefter går vi in på hur malware används idag med fokus på ett par av de hittills mest komplexa malwares som upptäckts; Stuxnet och Flame. Vi avslutar med en diskussion och sammanfattning kring virusens utveckling och syfte.

22. En studie om virus och trojaner i Windowsmiljö - med inriktning på polistrojanen

Henrik Skog, Mattias Mikkelä

Vi kommer att gå igenom hur virus och trojaner fungerar och även gå in lite djupare på Melissa-viruset. Vidare så förklarar vi vad ransomware är för något och lite historia om hur det började. Till sist handlar det om polistrojanen som började cirkulera och terrorisera detta året.

23. Digital ljudsteganografi med hjälp av LSB

Joakim Nymberg, Johan Oskarsson

I vårt projekt gömmer vi textmeddelande i ljudfiler (WAV) med hjälp av en mjukvara baserat på Least Significant Bit-metoden (LSB). Därefter tittar vi både binärt och frekvensmässigt hur mycket filerna förändras.

24. Forcering av hashade lösenord - Verktyg och tidsåtgång

Carl-Johan Hedenberg, Martin Björk

Vi skall titta på hur ett modernt verktyg för forcering av hashade lösenord ser ut och vad det använder för metoder. Vi kommer också att jämföra hur tidsåtgången för forcering kan komma att skilja sig mellan några vanliga kryptografiska hashfunktioner.

25. Utvärdering av lösenordsstrategier

David Jorlöv

Jag kommer i mitt projekt att utreda olika autentisering lösningar med skärkild inriktning på autentisering med hjälp av lösenord. Enligt min problem besrivning ska jag utreda varför ett svagt lösenord är ett problem och vad som är ett svagt lösenord. Samnt ge förslag på olika metoder att stärka dessa. Dessutom tänkte jag utreda om det är ett bra set att kombination av olika autentisering lösningar med lörsenord för att stärka svaga lörsenord.