**Unit-V: System Level Security**

**Session -1 Intrusion detection Date: 18.09.2013 Period: 05**

* **Unspoken words (Intruder Introduction)**

**www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch18.ppt**

1. Masquerader
2. Misfeasor
3. Clandestine user
* **Recall by keywords(Intrusion technique)**
* One-way encryption
* Access control
* **Recall by keywords (Intrusion Detection)**
* Statistical anomaly detection
* Counter
* Gauge
* Interval timer
* resource utilization
* Rule based detection
* Rule based anomaly detection
* Rule based penetration identification
* Audit records
* Detection –specific audit records
* Native audit records

**Session -2 Password management Date: 24.09.2013 Period: 03**

Presentation (**www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch18.ppt**)

Activity: Crossword



* **Quiz**
1. List and briefly define three classes of intruders.
2. What are two common techniques used to protect a password file?
3. What are three benefits that can be provided by an intrusion detection system?
4. What is the difference between statistical anomaly detection and rule-based intrusion detection?
5. What metrics are useful for profile-based intrusion detection?
6. What is the difference between rule-based anomaly detection and rule-based penetration identification?
7. What is a honeypot?
8. What is a salt in the context of UNIX password management?
9. List and briefly define four techniques used to avoid guessable passwords.

**Session -3 Viruses and Related threats Date: 08.10.13 Period: 06**

* Video: <http://www.youtube.com/watch?v=qy0-X7CTqss>

http://www.youtube.com/watch?v=c34QwtYI40g

* Presentation: (**www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch19.ppt)**
* Quiz
1. What is the role of compression in the operation of a virus?
2. What is the role of encryption in the operation of a virus?
3. What are typical phases of operation of a virus or worm?
4. In general terms, how does a worm propagate?
5. What is a digital immune system?
6. How does behavior-blocking software work?

**Session -4 Virus counter measures Date: 11.10.13 Period: 06**

Video: <http://www.youtube.com/watch?v=qy0-X7CTqss>

* Presentation (**www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch19.ppt)**
* Recall by keyword
* Antivirus approach
* Detection
* Identification
* Removal
* Quiz
1. How does a worm propagate?
2. What is the role of encryption in the operation of a virus?
3. What are the 4 generations of antivirus software?
4. Briefly describe the recent worm attack.
5. Why Morris worm is designed?

**Session -5 Digital immune system (DIS) Date: 12.10.13 Period: 03**

* **Recall by keyword**
1. CPU emulator
2. Virus signature scanner:
3. Emulation control module
* **Presentation** (**www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch19.ppt)**
* **Quiz**
1. What is a digital immune system?
2. How does behavior-blocking software work?
3. What is a DDoS?

**Session -6 Firewall design principles Date: 12.10.13 Period: 07**

* Show and tell

 



* **Presentation (http://ece.uprm.edu/~noack/crypto/textslides/ch20.ppt)**
* **Remember by keyword**
1. Service control
2. Direction control
3. User control
4. Behaviour control
* **Quiz**
1. List three design goals for a firewall.
2. List four techniques used by firewalls to control access and enforce a security policy.
3. What information is used by a typical packet-filtering router?
4. What are some weaknesses of a packet-filtering router?
5. What is the difference between a packet-filtering router and a stateful inspection firewall?
6. What is an application-level gateway?
7. What is a circuit-level gateway?

**Session -7 Firewall configuration Date: 17.10.13 Period: 05**

**Recall by words:**

 Screened host firewall system – single homed bastion host

 Screened host firewall system –dual homed bastion host

 Screened subnet firewall system

**Presentation: (http://ece.uprm.edu/~noack/crypto/textslides/ch20.ppt)**

**Session -8 Trusted Systems Date: 22.10.2013 Period:08**

**Presentation (**[**http://ece.uprm.edu/~noack/crypto/textslides/ch20.ppt**](http://ece.uprm.edu/~noack/crypto/textslides/ch20.ppt)**)**

**Conclusion:**

* **Quiz**
* In the context of access control, what is the difference between a subject and an object?

Subject: An entity capable of accessing objects, the concept of subject equates with that of process

Object: Anything to which access is controlled (e.g. files, programs)

* What is the difference between an access control list and a capability ticket?
	+ An access control list lists users and their permitted access right
	+ A capability ticket specifies authorized objects and operations for a user
* What are the two rules that a reference monitor enforces? N o read up, No write up
* What properties are required of a reference monitor?

Complete mediation, Isolation &Verifiability