Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: A **300 level** number requested**.**
2. Course Title: **Network and Web Application Security**
3. No. of Lectures per week: 0 (L), Tutorial: 1 (T), Laboratory: 3 (P), Additional Hours: 3 (A),

   Credits (3*L+2*T+P+A): 08 Duration of Course: Full Semester
4. Proposing Department/IDP : WSAIS

   Other Departments/IDPs which may be interested in the proposed course: CSE

   Other faculty members interested in teaching the course: Somitra Sanadhya, Manindra Agrawal
5. Proposing Instructor: DUGC (WSAIS)
6. Course Description:

A) Objectives: The objective of this practical-based course is to impart hands-on training in fundamentals of network and web security. The students will learn to manage firewalls, configure and manage VPN, control network traffic using applications and user identities, and develop real-world firewall administration and troubleshooting skills.

B) Contents: **(for 13 weeks of labs, tutorials, and additional work)**

S. No	Type	Title	Topics	Tools	Duration
1	Theory	**Network Perimeter Defense Fundamentals**	Network perimeter security defines the boundary between trusted internal networks and untrusted external networks. Firewalls enforce security controls at these boundaries by inspecting and filtering traffic. Stateless, stateful, and proxy firewalls differ in how deeply they analyze traffic and sessions.	Whiteboard + flow diagrams	1 Hour
	Practical		**Network Perimeter Analysis and Trust Boundary Identification** **Lab Objectives** 1. Understand how traffic flows across a network perimeter. 2. Identify trust boundaries within a simple network design. 3. Analyze choke points where security controls must be enforced. 4. Correlate firewall types with traffic inspection behavior		3 Hours

			Tasks 1. Study a given network diagram consisting of: o Internal LAN o DMZ o External (Internet) network 2. Trace packet flow from: o Internal LAN → Internet o Internet → Internal LAN 3. Identify: o Entry and exit points of traffic o Network perimeter locations 4. Mark trust boundaries between: o Trusted zone o Semi-trusted zone (DMZ) o Untrusted zone 5. Identify perimeter choke points where: o Firewalls o Proxy devices o Inspection controls should be placed 6. Analyze traffic handling differences for: o Stateless firewall (packet-by-packet) o Stateful firewall (session-aware) o Proxy firewall (application-level mediation) 7. Document observations on how each firewall type affects traffic flow.		

2	Theory	**Firewall Policy Design & Optimization**	Firewall policies control traffic flow using ordered rules based on source, destination, and service. A default-deny approach ensures only explicitly allowed traffic is permitted. Incorrect rule ordering can cause shadowing, conflicts, and unintended access.	Virtual firewall lab	1 Hour
	Practical		**Firewall Rule-Set Design, Optimization, and Traffic Analysis** **Lab Objectives** 1. Design firewall policies based on business requirements. 2. Understand the impact of rule ordering and implicit deny. 3. Identify and resolve rule shadowing and conflicts. 4. Analyze packet behavior with and without firewall rules. **Tasks** 1. Define a basic business requirement scenario: o LAN users accessing Internet services o Restricted inbound access from WAN 2. Design an initial firewall rule-set implementing: o Explicit allow rules o Implicit deny at the end 3. Configure firewall rules to allow: o Outbound traffic from LAN to WAN o Restricted inbound traffic from WAN to LAN		3 Hours

			4. Observe packet behavior: o With firewall enabled o Without firewall enabled 5. Verify the presence and effect of the **implicit deny rule**. 6. Create **explicit deny rules** and compare behavior with implicit deny. 7. Introduce misordered rules to demonstrate: o Rule shadowing o Rule conflicts 8. Optimize the firewall policy by: o Removing redundant rules o Reordering rules correctly 9. Capture traffic using packet capture tools. 10. Analyze captured packets in Wireshark to verify: o Allowed traffic o Blocked traffic o Rule hit behavior		
3	Theory	**Advanced Firewall Architectures**	Modern firewalls are deployed using advanced architectures for scalability and performance. Single-pass and multi-pass architectures differ in how traffic is inspected across security engines. Security zones logically segment networks to simplify policy enforcement and reduce risk.	Virtual lab network	1 Hour

	Practical		**Firewall Zoning and Advanced Architecture Implementation** **Lab Objectives** 1. Understand advanced firewall deployment architectures. 2. Implement logical network segmentation using security zones. 3. Differentiate Layer 2 and Layer 3 firewall zones. 4. Relate firewall architecture to traffic inspection efficiency. **Tasks** 1. Design a virtual network consisting of: o Internal network o DMZ o External network 2. Logically divide the network into security zones. 3. Assign trust levels to each zone. 4. Configure: o Layer 2 zones (same subnet segmentation) o Layer 3 zones (routed segmentation) 5. Define traffic flow rules between zones. 6. Observe traffic inspection behavior in: o Single-pass firewall architecture o Multi-pass firewall architecture 7. Compare performance and inspection logic between architectures. 8. Validate zone-based access control by testing: o Allowed inter-zone traffic o Blocked inter-		3 Hours

			zone traffic 9. Document how zoning simplifies firewall policy management.		
4	Theory	**ACLs & Network Traffic Control**	Access Control Lists (ACLs are basic filtering mechanisms applied on routers or interfaces. ACLs evaluate traffic using IP addresses, protocols, and port numbers. Protocols like ICMP and Telnet increase risk due to limited control and lack of encryption.	Router / firewall emulator	1 Hour
	Practical		**Access Control Lists (ACL) Configuration and Traffic Validation** **Lab Objectives** 1. Understand how ACLs control network traffic. 2. Block insecure protocols using router-based ACLs. 3. Validate allowed and denied traffic using packet analysis. 4. Compare ACL-based control with firewall rule behavior **Tasks** 1. Configure a basic router with LAN and WAN interfaces. 2. Identify insecure protocols such as: o ICMP o Telnet 3. Create ACL rules to: o Block Telnet traffic o Restrict ICMP traffic as per requirement 4. Apply ACLs to the appropriate router interface and direction. 5. Generate traffic from a client machine using blocked protocols. 6. Capture traffic using Wireshark. 7. Verify blocked traffic		3 Hours

			does not pass the router. 8. Generate secure traffic (e.g., HTTPS or SSH). 9. Validate allowed traffic using packet capture. 10. Compare behavior of: o Router ACL rules o Firewall-based security rules 11. Document differences in control granularity and inspection depth.		
5	Theory	**VPN Concepts & Enterprise Use-Cases**	Virtual Private Networks (VPNs) provide secure communication over untrusted networks. Site-to-site VPNs connect entire networks, while remote-access VPNs support individual users. Tunneling encapsulates private traffic to maintain confidentiality and integrity.	Manual threat modelling	1 Hour
	Practical		**Site-to-Site VPN Deployment and Routing Configuration Lab Objectives** 1. Understand enterprise VPN use-cases. 2. Configure a site-to-site VPN between two networks. 3. Implement routing required for VPN traffic flow. 4. Analyze trust boundaries across VPN tunnels. **Tasks** 1. Design two separate network sites with distinct subnets. 2. Configure routing between internal networks at both sites. 3. Configure a site-to-site VPN tunnel on the router. 4. Define local and remote encryption domains. 5. Install required routing		3 Hours

			and VPN modules on a Windows Server. 6. Verify tunnel establishment. 7. Generate traffic between Site A and Site B. 8. Validate that traffic flows through the VPN tunnel. 9. Confirm that tunneled traffic is inaccessible from outside networks. 10. Document routing and tunnel behavior.		
6	Theory	**IPsec Architecture & Key Management**	IPsec secures network traffic using encryption, authentication, and integrity checks. ISAKMP and IKE protocols manage secure key exchange using IKEv1 or IKEv2. Security Associations define how traffic is protected between communicating peers.	VPN + PCAP tools	1 Hour
	Practical		**IPsec Tunnel Design, Key Exchange, and Traffic Validation** **Lab Objectives** 1. Understand IPsec architecture and key exchange mechanisms. 2. Configure IPsec tunnels using secure parameters. 3. Validate encrypted traffic flow. 4. Differentiate encrypted and unencrypted traffic. **Tasks** 1. Configure an IPsec VPN tunnel on a firewall. 2. Define ISAKMP/IKE parameters: o Encryption o Authentication o Key lifetime 3. Establish the IPsec tunnel. 4. Generate traffic between protected		3 Hours

			networks. 5. Capture traffic using packet capture tools. 6. Identify encrypted IPsec packets in captures. 7. Compare traffic before and after IPsec encryption. 8. Validate successful key negotiation. 9. Document encryption behavior and tunnel stability.		
7	Theory	**Application Awareness & Control**	Port-based firewall rules are insufficient for modern web applications. Application-aware firewalls identify traffic using application signatures. This allows granular control over specific applications and sub-application functions.	AppID	1 Hour
	Practical		Configure the firewall to allow general web browsing but specifically block "Sub-Applications" like Facebook Games or File Uploads within LinkedIn. **Application-Based Firewall Policy Enforcement** **Lab Objectives** 1. Move from port-based filtering to application-based control. 2. Control sub-application behavior within allowed applications. 3. Enforce granular access policies using application signatures. **Tasks** 1. Configure firewall application identification features. 2. Allow general web browsing traffic. 3. Create application-based rules to: o Allow		3 Hours

			LinkedIn browsing o Block LinkedIn file uploads 4. Create rules to: o Allow Facebook access o Block Facebook games 5. Test access from a client browser. 6. Verify allowed application functions. 7. Verify blocked sub-application behavior. 8. Analyze logs to confirm application-level detection. 9. Document differences between port-based and application-based filtering. **Tasks** 1. Configure firewall application identification features. 2. Allow general web browsing traffic. 3. Create application-based rules to: o Allow LinkedIn browsing o Block LinkedIn file uploads 4. Create rules to: o Allow Facebook access o Block Facebook games 5. Test access from a client browser. 6. Verify allowed application functions. 7. Verify blocked sub-application behavior. 8. Analyze logs to confirm application-level detection. 9. Document differences		

			between port-based and application-based filtering.		
8	Theory	**SSL/TLS Inspection (Man-in-the-Middle)**	Encrypted SSL/TLS traffic bypasses traditional firewall inspection. SSL/TLS inspection decrypts traffic, applies security checks, and re-encrypts it. This enables detection of threats hidden within encrypted sessions.	ngfw	1 Hour
	Practical		**HTTPS Decryption and Encrypted Traffic Inspection Lab Objectives** 1. Understand how SSL/TLS inspection works. 2. Configure a firewall to decrypt HTTPS traffic. 3. Inspect encrypted traffic for restricted content. 4. Analyze the impact of TLS inspection on traffic visibility. **Tasks** 1. Generate a local Certificate Authority (CA) certificate. 2. Install the CA certificate on a client machine. 3. Configure the firewall for SSL/TLS inspection. 4. Enable HTTPS decryption for outbound traffic. 5. Define inspection rules for: o Restricted keywords o Malware signatures 6. Access HTTPS websites from the client. 7. Verify decrypted		3 Hours

			traffic inspection on the firewall. 8. Validate blocked content based on inspection rules. 9. Confirm re-encryption of traffic before forwarding. 10. Document inspection results and security implications.		
9	Theory	**Intrusion Prevention System (IPS) Tuning**	Intrusion Detection Systems (IDS) generate alerts for suspicious traffic. Intrusion Prevention Systems (IPS) actively block confirmed attacks. Proper tuning is required to prevent false positives while stopping real threats.	ngfw	1 Hour
	Practical		**IPS Detection, Prevention, and Signature Tuning** **Lab Objectives** 1. Distinguish between IDS and IPS operational modes. 2. Detect application-layer attacks. 3. Tune IPS rules to reduce false positives. 4. Actively prevent confirmed attacks. **Tasks** 1. Deploy an internal web server. 2. Configure Suricata or Snort in detection (IDS) mode. 3. Launch a SQL Injection attack against the server. 4. Observe alerts without traffic blocking. 5. Switch IPS to prevention mode. 6. Re-launch SQL Injection or XSS attack. 7. Verify that malicious packets are dropped. 8. Analyze IPS logs for triggered signatures. 9. Adjust rules to reduce		3 Hours

			false positives. 10. Validate normal traffic remains unaffected.		
10	Theory	**User-ID & Identity-Based Policies**	IP-based policies cannot reliably identify individual users. User-ID integrates firewalls with identity systems like Active Directory or LDAP. Policies can then be enforced based on users or groups instead of IP addresses.	Windows Server (AD), ngfw.	1 Hour
	Practical		**Identity-Based Firewall Policy Enforcement Using Active Directory** **Lab Objectives** 1. Integrate firewall policies with user identities. 2. Apply access control based on AD group membership. 3. Enforce security policies beyond IP-based rules. **Tasks** 1. Integrate firewall with Active Directory using LDAP. 2. Verify successful user authentication mapping. 3. Create AD groups: o Accounting o IT 4. Create firewall rules to: o Allow Accounting group access to QuickBooks Online o Deny IT group access to QuickBooks Online		3 Hours

			5. Test access from users belonging to each group. 6. Verify correct policy enforcement. 7. Review logs showing user-based rule matches. 8. Document identity-based policy behavior.		
11	Theory	**Geolocation-Based Filtering**	Geolocation filtering restricts traffic based on the country of origin. It reduces exposure to attacks from high-risk regions. This technique is commonly used for inbound threat mitigation.	ngfw	1 Hour
	Practical		**Geolocation-Based Traffic Filtering Using Country Databases** **Lab Objectives** 1. Reduce attack surface using geographic controls. 2. Implement location-based blocking rules. 3. Validate geolocation filtering effectiveness. **Tasks** 1. Import MaxMind geolocation databases into the firewall. 2. Create an alias containing high-risk countries. 3. Configure firewall rules to: o Drop unsolicited inbound traffic from those regions 4. Generate simulated inbound traffic. 5. Verify blocked traffic based on geographic origin. 6. Analyze firewall logs for country-based filtering. 7. Validate legitimate traffic from allowed		3 Hours

			regions. 8. Document geolocation filtering outcomes.		
12	Theory	**URL Filtering & Web Reputation**	URL filtering categorizes websites based on content and risk. Web reputation scores indicate the trustworthiness of a website. Firewalls block access to malicious or low-reputation URLs automatically.	ngfw	1 Hour
	Practical		**Web Access Control Using URL Categories and Reputation Scores** **Lab Objectives** 1. Protect users from malicious web content. 2. Enforce category-based browsing restrictions. 3. Block low-reputation URLs automatically. **Tasks** 1. Enable URL filtering on the firewall. 2. Configure category-based blocking for: o Gambling o Hate Speech o Phishing 3. Configure reputation-based rules. 4. Access blocked category websites from a client. 5. Verify access denial. 6. Click a low-reputation link. 7. Observe firewall response and logging. 8. Validate allowed access to permitted categories. 9. Document filtering behavior and user protection benefits.		3 Hours

13	Theory	**Zero Trust Network Access (ZTNA) Simulation**	Zero Trust assumes no implicit trust for users or devices. Authentication and authorization are required before any access is granted. Resources remain invisible until identity and policy checks are satisfied.	wildfire	1 Hour
	Practical		**Zero Trust Access Enforcement Using Reverse Proxy and MFA** **Lab Objectives** 1. Implement Zero Trust access principles. 2. Eliminate direct network exposure of internal resources. 3. Enforce identity-first access control. **Tasks** 1. Deploy an internal application not exposed to the internet. 2. Configure a reverse proxy in front of the application. 3. Integrate MFA with OIDC or SAML authentication. 4. Ensure unauthenticated users cannot discover the resource. 5. Authenticate a user through the identity provider. 6. Allow access only after successful authentication. 7. Verify denied access for unauthenticated requests. 8. Analyze logs for authentication and access decisions. 9. Document how ZTNA differs from traditional VPN access.		3 Hours

C) Pre-requisites:

- Basic understanding of computer networks (IP, TCP/IP, ports, protocols)
- Working knowledge of Windows and Linux OS
- Familiarity with networking devices like routers and switches
- Introductory cyber security knowledge

D) Short summary for including in the Courses of Study Booklet: This course imparts hands-on training to the students on the fundamentals of web and network security. The students will understand network perimeter security, design and implement firewall policies, analyze and control networks, applications, and user generated traffic. They will learn techniques to protect organizations from modern network based attacks.

7. Recommended books:
   • Tools which will be used are already listed in the weekly description.

Dated: 13 August 2026; Proposer: DUGC, WSAIS

Dated: ; DUGC Convener (WSAIS):_____

The course is approved / not approved

_____

Chairperson, SUGC

Dated:_____