PREPARING FOR A HACK & RECONNAISSANCE

Information Gathering & Strategy for Cyber Resilience

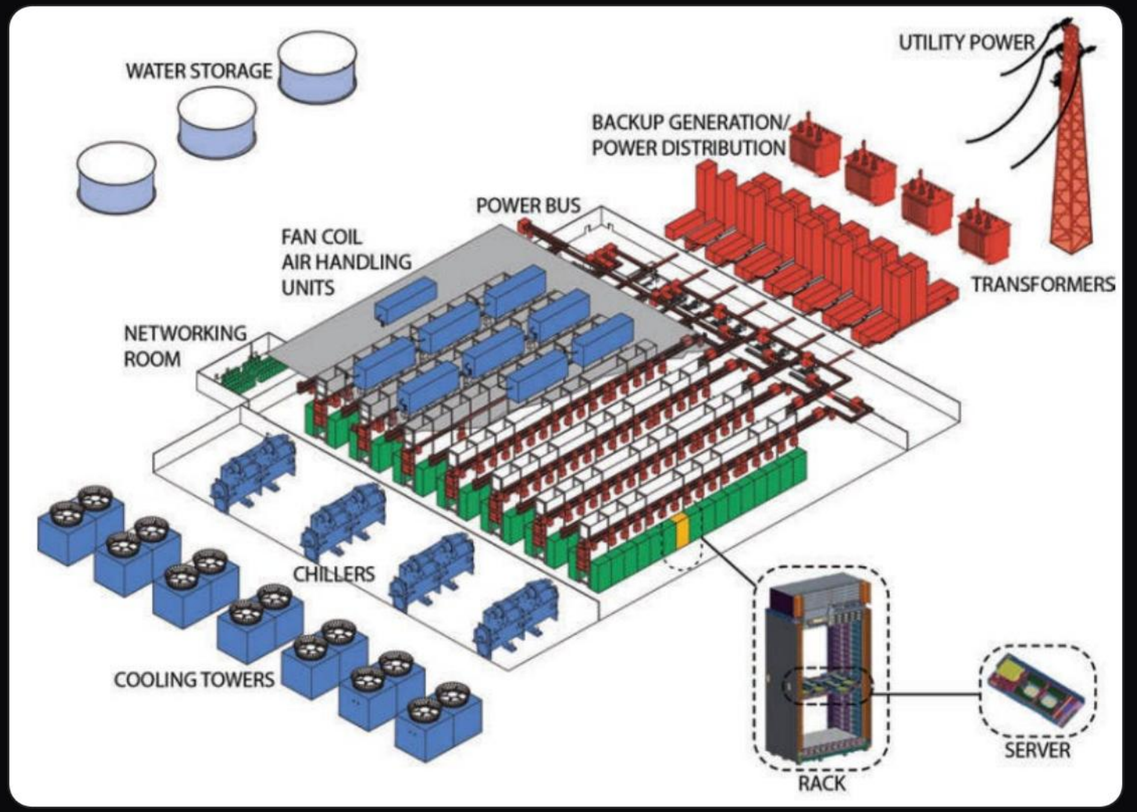
- Technical Prep
- Engagement Management
- Recon Techniques
- Social Engineering
- Physical Security
- Internet OSINT

Course: Ethical Hacking / Cyber Security | Module 02

Technical Preparation

- **Scope Definition:** Clearly set testing objectives and boundaries.
- **Authorization:** Obtain formal written approvals before any action.
- **Targeting:** Identify specific IP ranges and network assets.
- **Tooling:** Prepare frameworks and exploit environments.
- **Recovery:** Verify backup systems are operational.
- **Communication:** Establish channels for emergency response.

Goal: Safe execution without business disruption.



Managing the Engagement

Strategic Framework

- ✓ Develop detailed test plans & milestones.
- ✓ Define Rules of Engagement (RoE).
- ✓ Assign distinct roles and responsibilities.
- ✓ Monitor activities & provide status updates.

Engagement Benefits

- Optimized team coordination
- Drastically reduced operational risk
- High-precision reporting and audit trails

Reconnaissance Techniques

"Reconnaissance is the foundation of every successful attack."

Social Engineering

- Phishing & Vishing attacks
- Pretexting & Impersonation
- Psychological manipulation

Physical Security

- Access control evaluation
- Badge cloning & Tailgating
- Visitor management review

Technical Intel

- System fingerprinting
- Port scanning enumeration
- Service identification

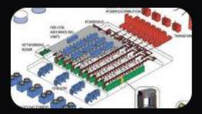
Internet Reconnaissance

- **DNS & WHOIS:** Domain enumeration and registrant details.
- **Google Dorking:** Advanced search reconnaissance for leaks.
- **Social Media:** Human intelligence (HUMINT) gathering.
- **Fingerprinting:** Identifying tech stacks and headers.

Why OSINT Matters?

Reveals exposed sensitive data and maps potential attack vectors before a single packet is sent to the target network.

Image Sources



https://substackcdn.com/image/fetch/f_auto,q_auto:good,fl_progressive:steep/https%3A%2F%2Fsubstack-post-media.s3.amazonaws.com%2Fpublic%2Fimages%2F9d6d3100-bd96-4454-8730-b48a5216a044_794x574.png

Source: www.construction-physics.com

https://static.vecteezy.com/system/resources/previews/070/084/660/large_2x/business-marketing-strategy-concept-with-digital-icons-analytics-charts-and-sales-growth-reports-symbolizing-online-promotion-target-audience-engagement-and-e-commerce-success-free-photo.jpg

Source: www.vecteezy.com

Thumbnail for osintteam.blog

https://miro.medium.com/1*X_L75nSrTEFASUN4dIf4Dw.png

Source: osintteam.blog

https://images.squarespace-cdn.com/content/v1/65a6addd51274933815f8a83/17c8bb73-db3d-44e2-86e2-b3916970f59b/AP.png

Source: www.cybersecurityinsights.us